山东大学
SHANDONG UNIVERSITY

# TrojPix: Electromagnetic Covert Channels via Imperceptible Pixel Modulation

Guoming Zhang[1, 2], Huiting Zhang[1], Zhenwei Lu[1], Heqiang Fu[1], Xin Gao[1], Riccardo Spolaor[1], Yetong Cao[1, 2], Yanni Yang[1, 2], and Pengfei Hu[1, 2*]

*Shandong University · Quan Cheng Laboratory*

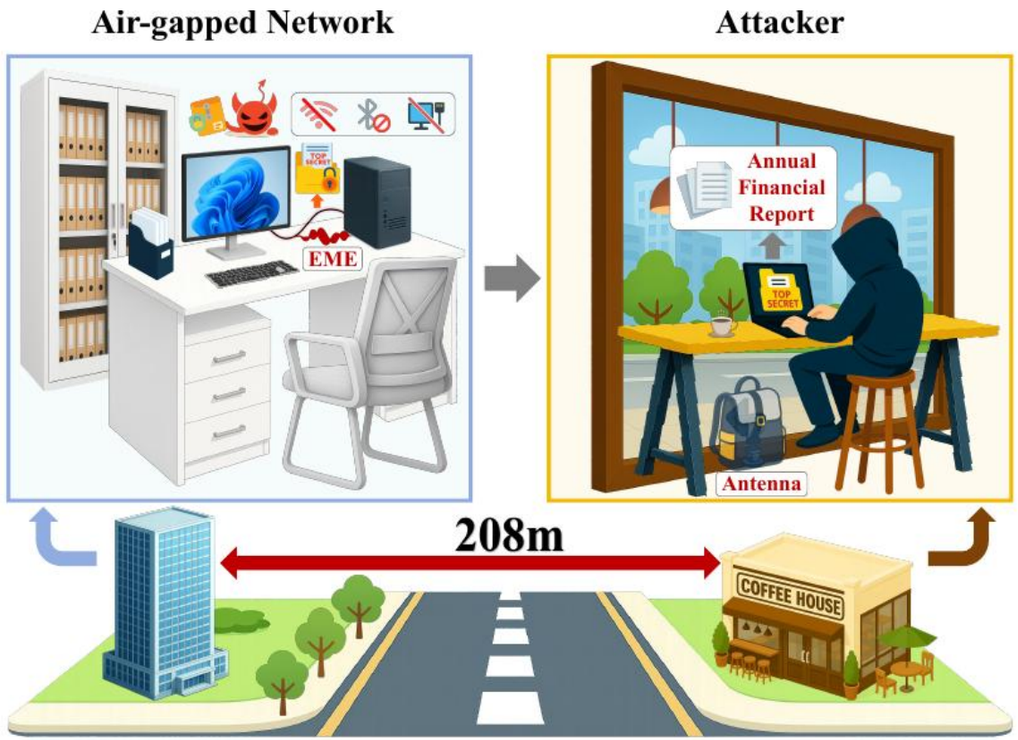
Presented by Huiting Zhang, China.

## Data Exfiltration from Air-Gapped Networks

- Air-gapped systems prohibit direct network communication
- Malware can manipulate unintended physical emissions
- Remote attackers may recover sensitive information across the isolation boundary

## Attack Scenario

- Malware-infected computer
- Imperceptible display manipulation
- Electromagnetic leakage
- Remote signal reception
- Sensitive-data recovery



## Limitations of Existing Methods

- Low transmission rate
- Limited communication range
- Poor visual stealth

**TrojPix**

**8.1 Mbps**

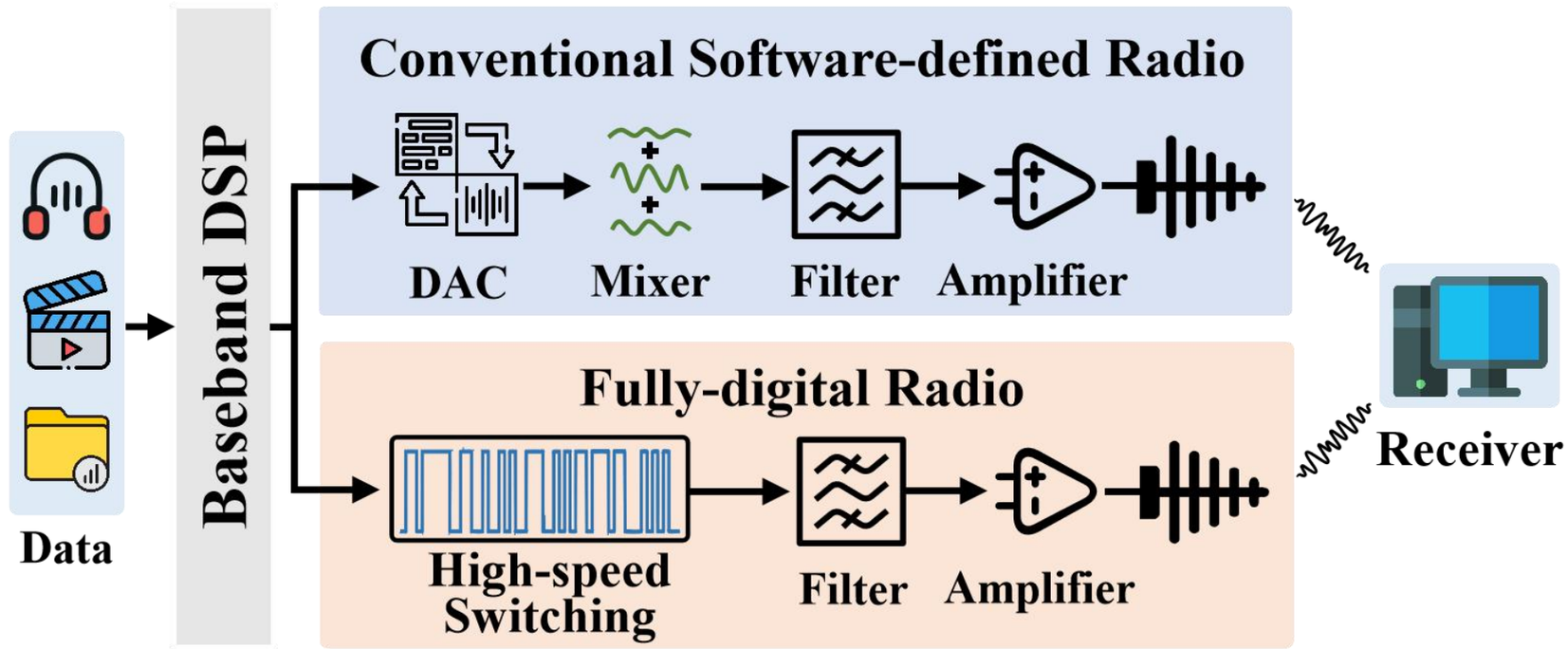
**208 m**

- **Visually imperceptible**
- **High Speed**
- **Long Distance**

**27× faster than the prior peak rate**
**2.38× the prior longest range**

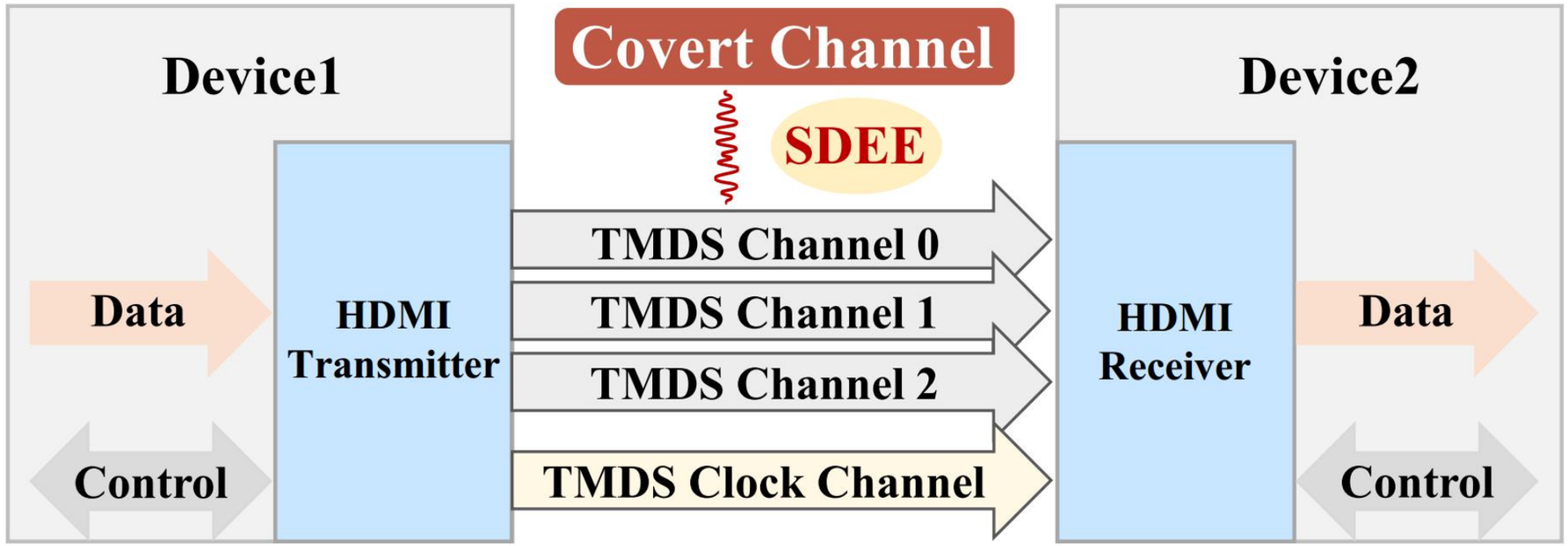
# Fully-Digital Radios

- RF generation via high-speed switching
- Fewer analog components
- Digital interfaces as RF sources



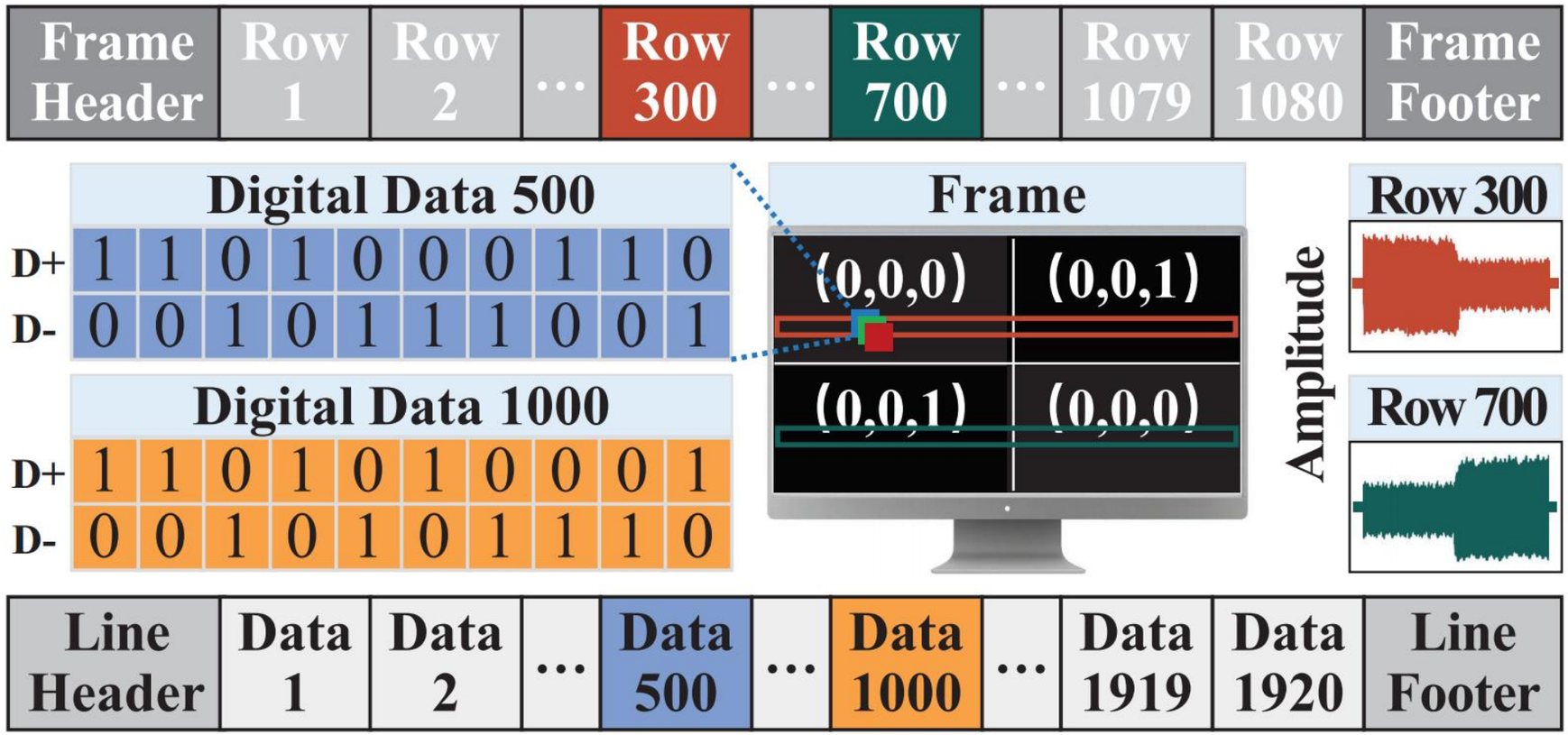
# Background

- High-speed TMDS switching induces EM radiation
- Video cables act as unintended antennas
- Pixel data can shape leakage for covert communication

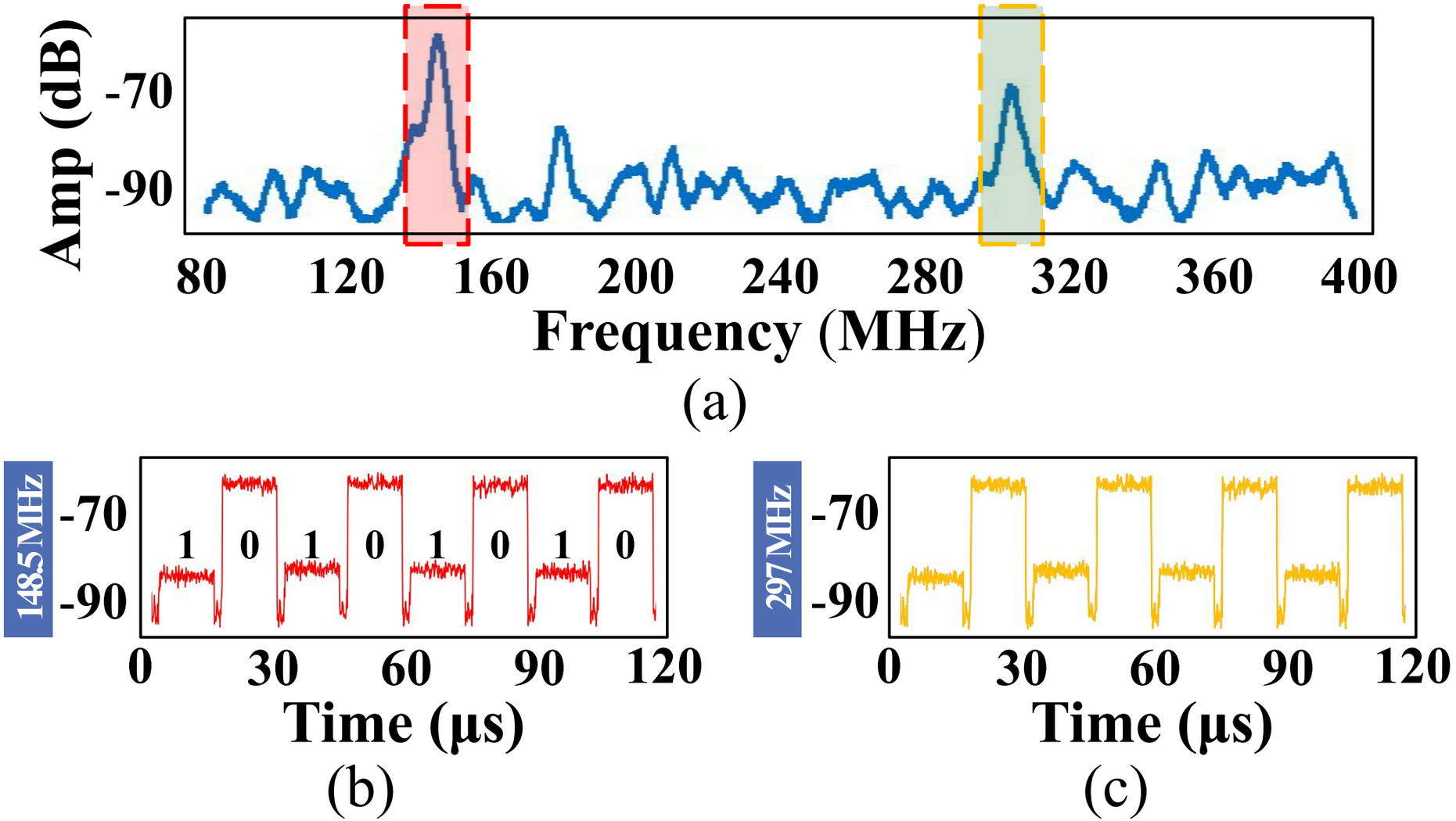


# Feasibility Analysis

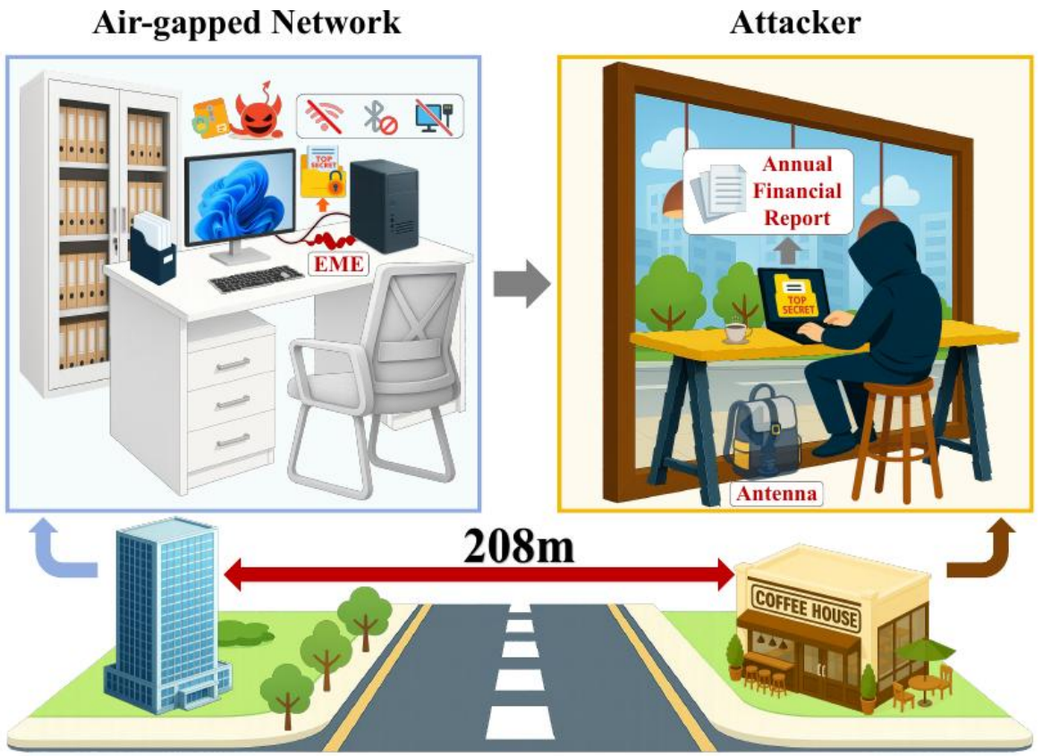
Illustration of EM signal variations induced by pixel modifications.



Demonstration of covert information transmission on different frequency bands.



# Threat Model




## Attacker Capabilities

- user-mode malware
- no admin rights
- no peripheral access
- remote SDR receiver

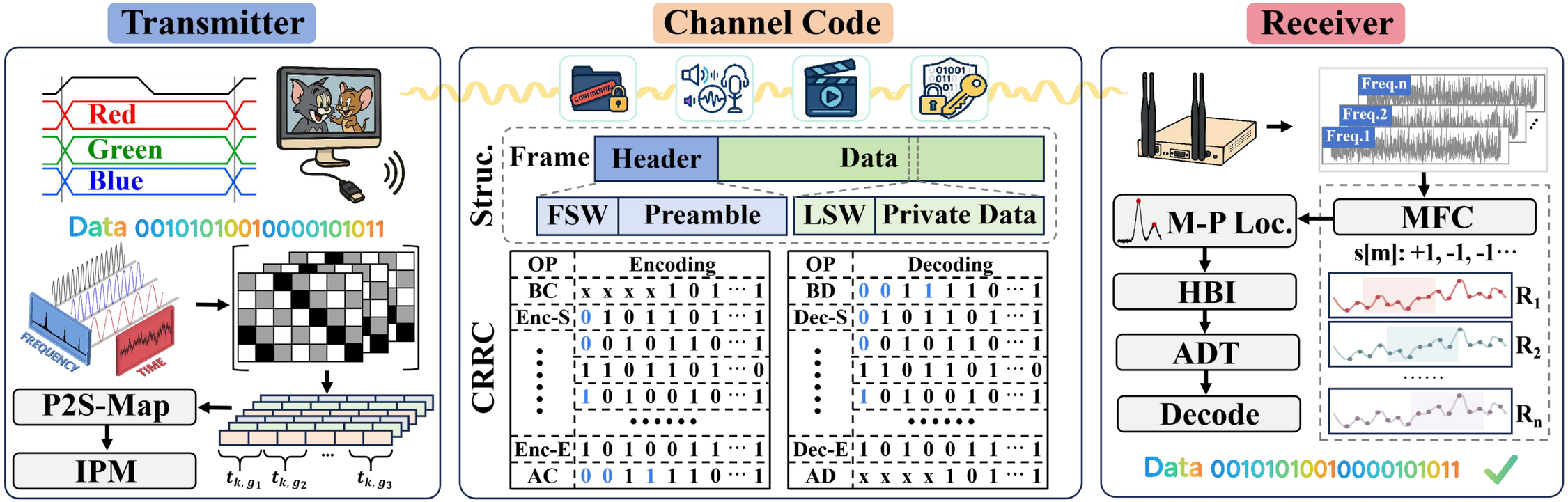
### 1 FAKE SCREEN-OFF

The display appears off while covert transmission continues.

### 2 FOREGROUND EMBEDDING

Data is embedded into normal content via imperceptible pixel changes.

# TrojPix System Overview




**Transmitter:** Maps data to pixels with imperceptible modulation.

**Channel Coding:** Frames and encodes data for robust transmission.

**Receiver:** Synchronizes, fuses, and decodes EM signals.

## Intra–Row OOK Modulation

$$L_{k,m}^{(1)}=\begin{cases}\text{clip}(L_{k,m}^{(0)}+\delta), & b_g=1,\ (k,m)\in X_{\text{sym}}(g),\\ L_{k,m}^{(0)}, & b_g=0\end{cases}$$

## Inter–Row Differencing

$$(L_{2u,m}^{(1)}, L_{2u+1,m}^{(1)})=\begin{cases}(\text{clip}(L_{2u,m}^{(0)}+\delta), \text{clip}(L_{2u+1,m}^{(0)}-\delta)), & b_g=1,\\ (L_{2u,m}^{(0)}, L_{2u+1,m}^{(0)}), & b_g=0,\end{cases}$$

**Matched-filter correlation finds the preamble**

**HBI recovers row boundaries**

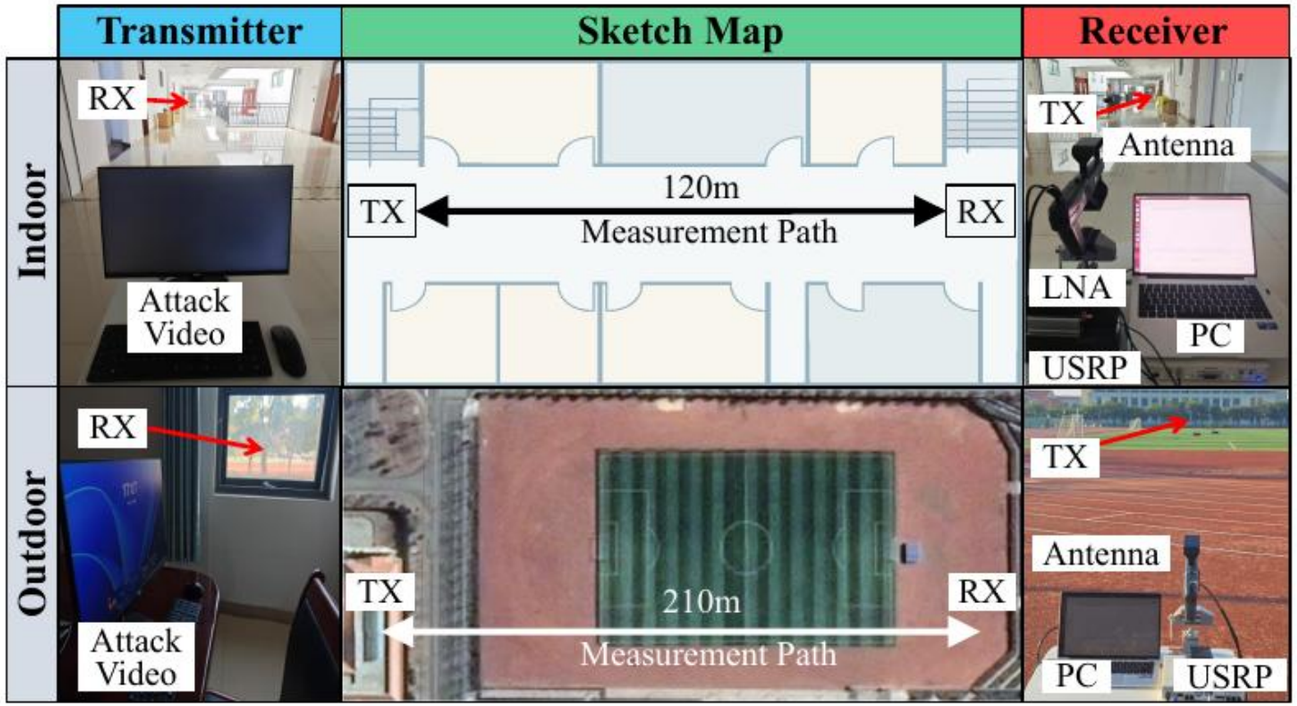
**ADT tracks the current channel**

$$\hat{b}_i = \mathbf{1}\{\, \text{flag} \cdot \quad (v_i - T_t) > 0 \,\}$$

$$\hat{m} = \text{Decode}\big(\text{DeInterleave}(\hat{b})\big)$$

The receiver is lightweight, but every stage is channel-aware.

# Evaluation Settings




## Settings

- Dell U2417H display
- 1920×1080 @ 60 Hz
- USRP X310 receiver
- ATFNW3 directional antenna
- Low-noise amplifier
- 10 MHz sampling rate

## Metrics

BCR / SNR / SSIM / LPIPS

12 monitors / 9 brands  15 cables / 8 brands

# Evaluation Results

山东大学 SHANDONG UNIVERSITY

**8.1 Mbps**

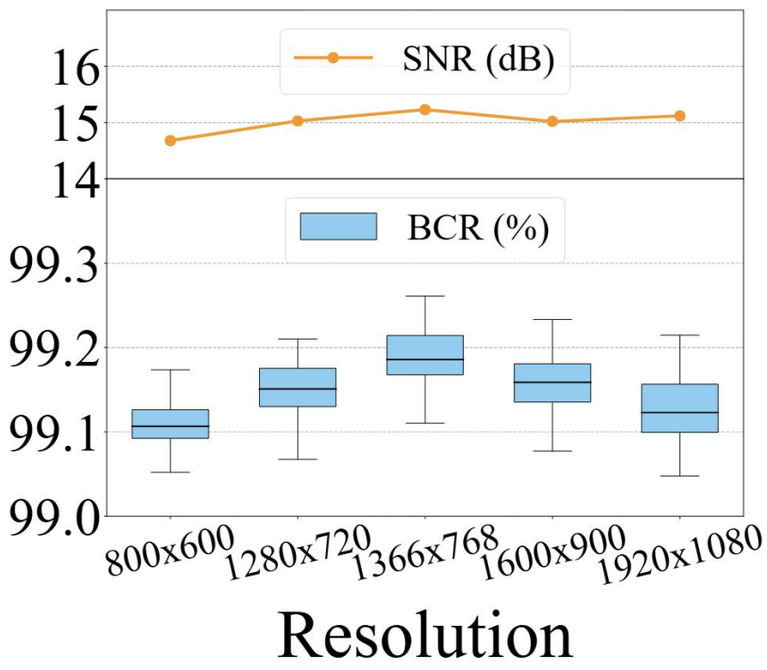
peak rate at 20 MHz sampling

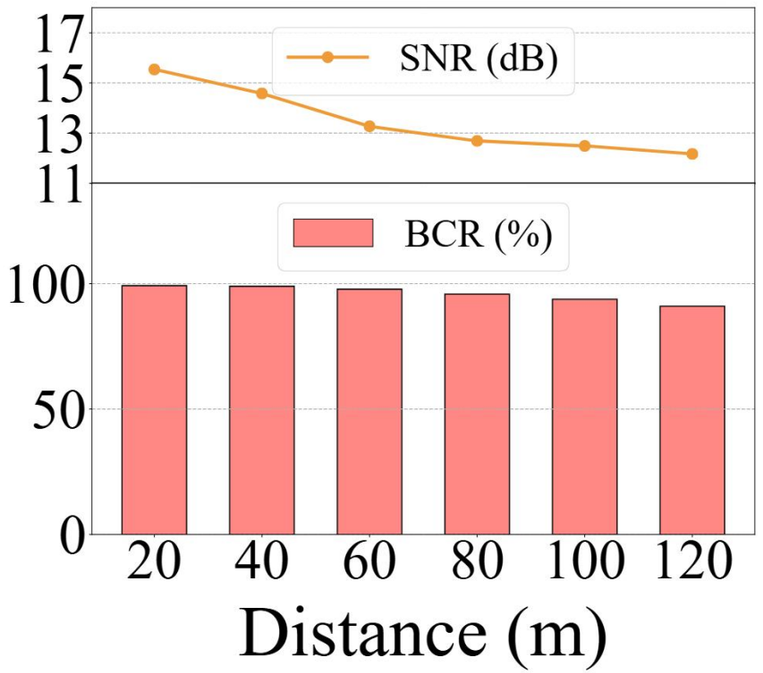
**208 m**

complete packet recovered

**99.14%**

average BCR through a 30 cm concrete wall



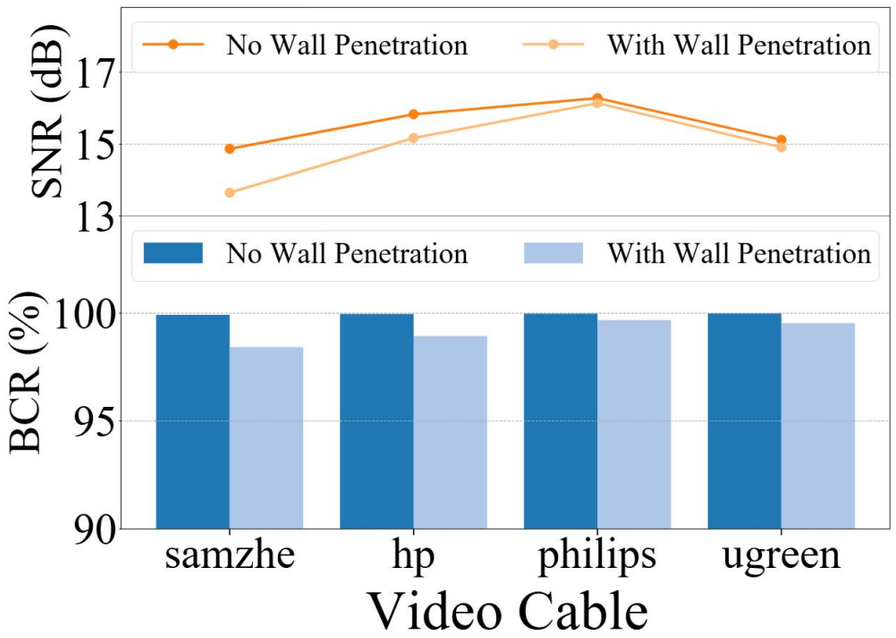



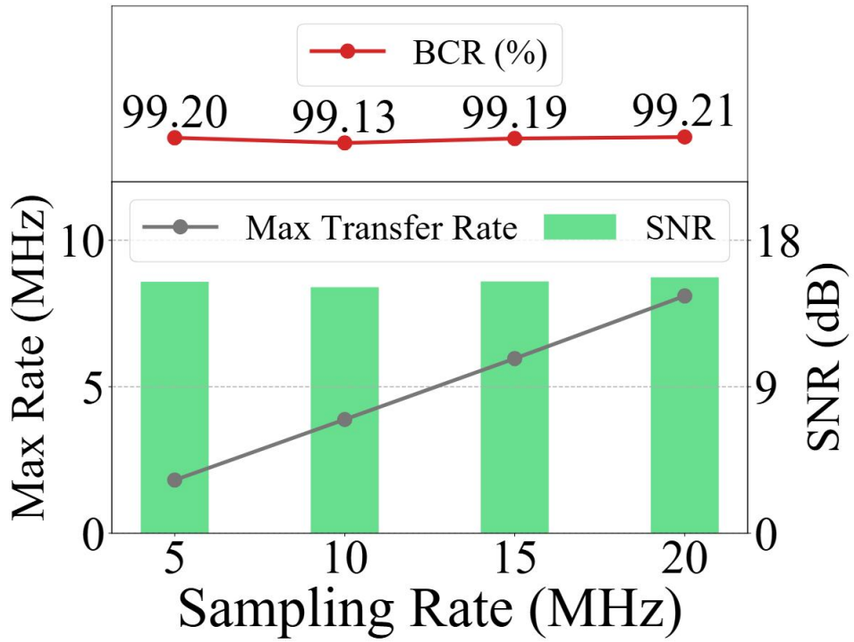
# Evaluation Results

**8.1 Mbps**
peak rate at 20 MHz sampling

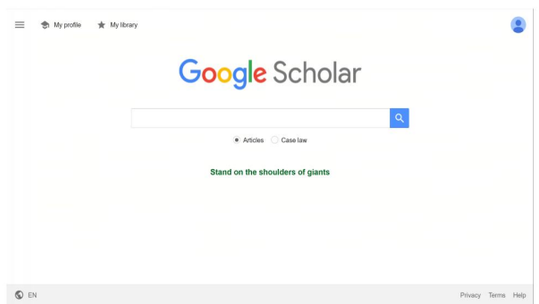
**208 m**
complete packet recovered

**99.14%**
average BCR through
a 30 cm concrete wall



# Evaluation Results




(a) Source image (webpage)




(b) Reconstructed image from (a)



(c) Source image (natural scene)




(d) Reconstructed image from (c)

**SSIM** **0.998 / 0.999**

webpage / natural scene

**LPIPS** **0.002 / 0.005**

webpage / natural scene

**BCR** **99.82% / 99.36%**

under textured content

**User study** **50 / 50**

reported no visible change

**The pixels change; the scene does not appear to.**

# Defense and Limitations

## Defense Strategies

- EM shielding
- Pixel-modulation detection
- Display-access control

## Limitations

- Requires malware
- SNR degradation

Best long-term fix: reduce or decorrelate display-interface emissions

# Thank you — Q&A

## TrojPix: Electromagnetic Covert Channels via Imperceptible Pixel Modulation

Guoming Zhang[1, 2], Huiting Zhang[1], Zhenwei Lu[1], Heqiang Fu[1], Xin Gao[1], Riccardo Spolaor[1], Yetong Cao[1, 2], Yanni Yang[1, 2], and Pengfei Hu[1, 2*]

*Shandong University · Quan Cheng Laboratory*

Presented by Huiting Zhang, China.