SCREEN2AIR

Air-Gap Exfiltration via High-Order Modulation-Based Screen Saver Covert Channels

Sungshin Women's University
Ye-Rim Jeong | Yeon-Jin Kim | Chea-Yeon Park | Il-Gu Lee
220254016@sungshin.ac.kr

Author Introduction

Ye-Rim Jeong | M.S in Convergence Security Engineering, Sungshin Women's University, Seoul, Korea

Key Achievements

- **Best Poster Award** in WISA 2025 (World Conference on Information Security Applications)
- **Best Paper Award** in The 8th Subchannel Information Analysis Contest 2025
- **Best Poster Award** in Mobisec 2024 (The 8th International Conference on Mobile Internet Security)

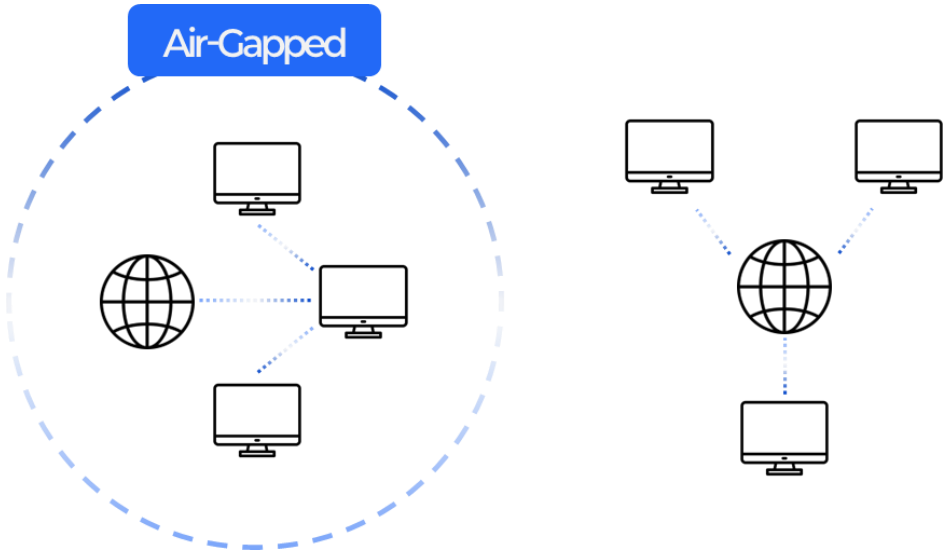
Research Interests

- Network Security and Threat Mitigation
- Network Performance Optimization
- IoT Security & Embedded Systems

Contact

- E-Mail: 220254016@sungshin.ac.kr
- https://sites.google.com/view/yerim-jeong

Background: Air-Gapped



Air-Gapped System

- Complete Physical Isolation between internal systems and external networks
  → **Prevents remote intrusion and data leakage**
- Used in critical infrastructure and military systems

Rethinking Air-Gap Security: A Call for Systematic Research

- Recent studies actively explore covert data leakage using EM, light, and mechanical vibrations
- Conventional defense cannot monitor such out-of-band communication paths
  → **Necessitates preemptive and systematic research on air-gap attack vectors**

Air-Gap Exfiltration via High-Order Modulation-Based Screen Saver Covert Channels

Related Work

Embedding QR codes into images [1]

1. Limited effective range depending on camera type

2. Potentially noticeable to users due to visual sensitivity

Air-Gapped Exploitation through Display

Utilizing the IR functionality of smart lighting systems [2]

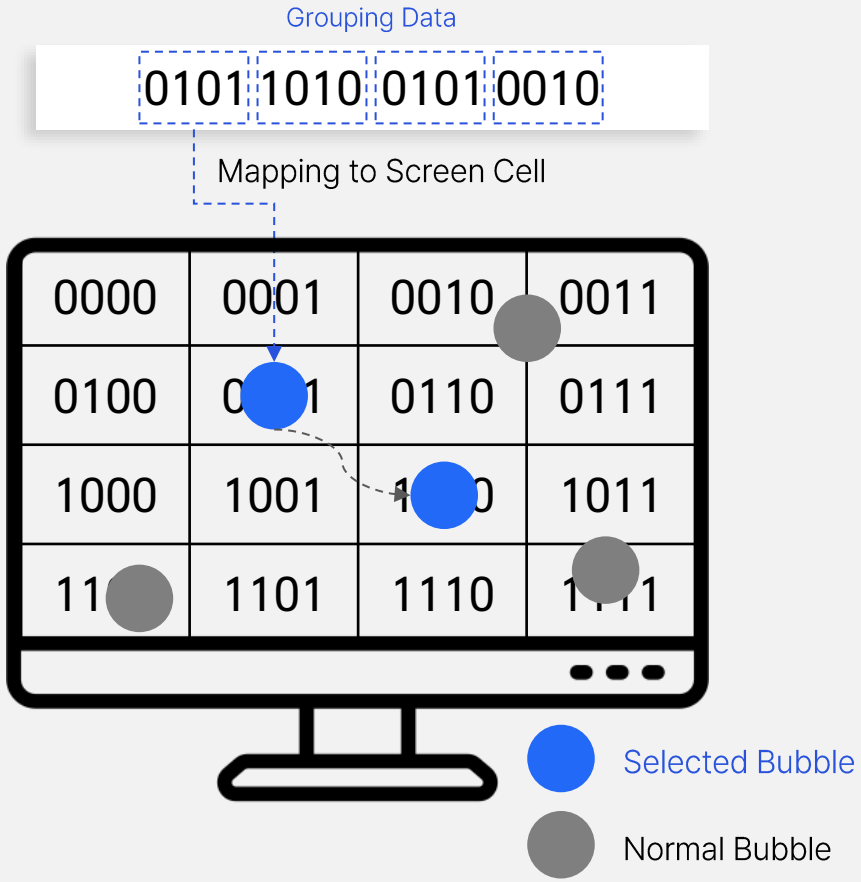
1. Depends on infrared-capable lighting, restricting real-world applicability

limited range and visible patterns → Low practicality

[1] Guri, M.: Optical air-gap exfiltration attack via invisible images. J. Inf. Secur. Appl. 46, 222–230 (2019).

[2] Maiti, A., Jadliwala, M.: Light ears: Information leakage via smart lights. Proc. ACM In-teract. Mob. Wearable Ubiquitous Technol. 3(3), 1–27 (2019)

Proposed Attack Model



Data Encoding

- Malware collects sensitive data → converts to binary (grouped into n-bit blocks)
- Map each n-bit block to one of 2^n screen cells

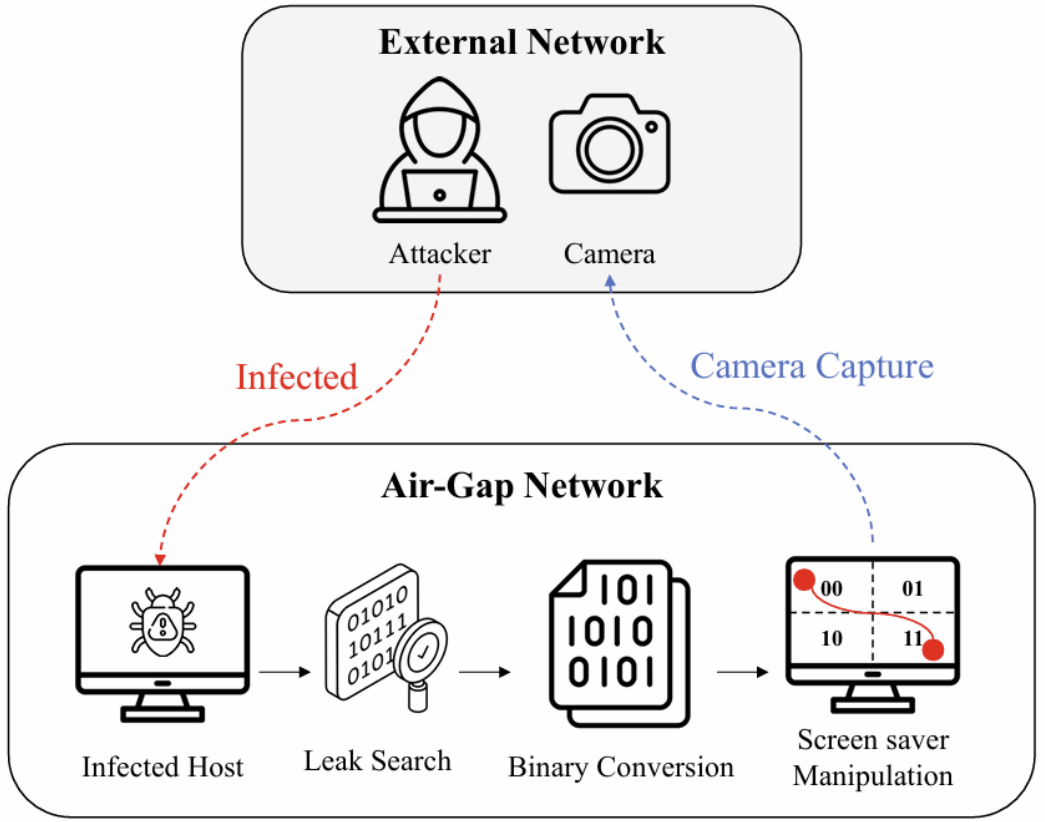
Data Transmission

- Selected bubble moves to the target cell and pauses
- Other bubbles move normally; external attacker decodes data from positions.

Proposed Attack Model

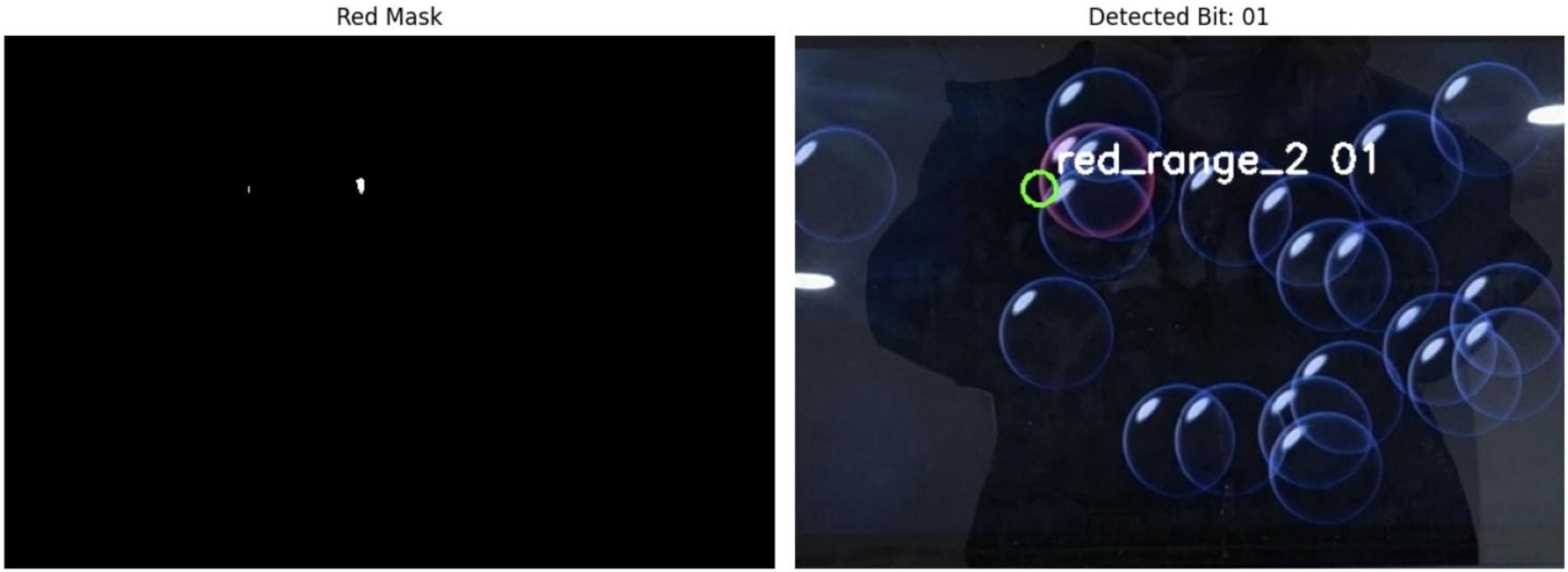
Key Features

- Hidden attacker-only marker among normal elements
- Operates during user absence → **Difficult to detect**
- Applicable to various visuals, range up to tens of meters



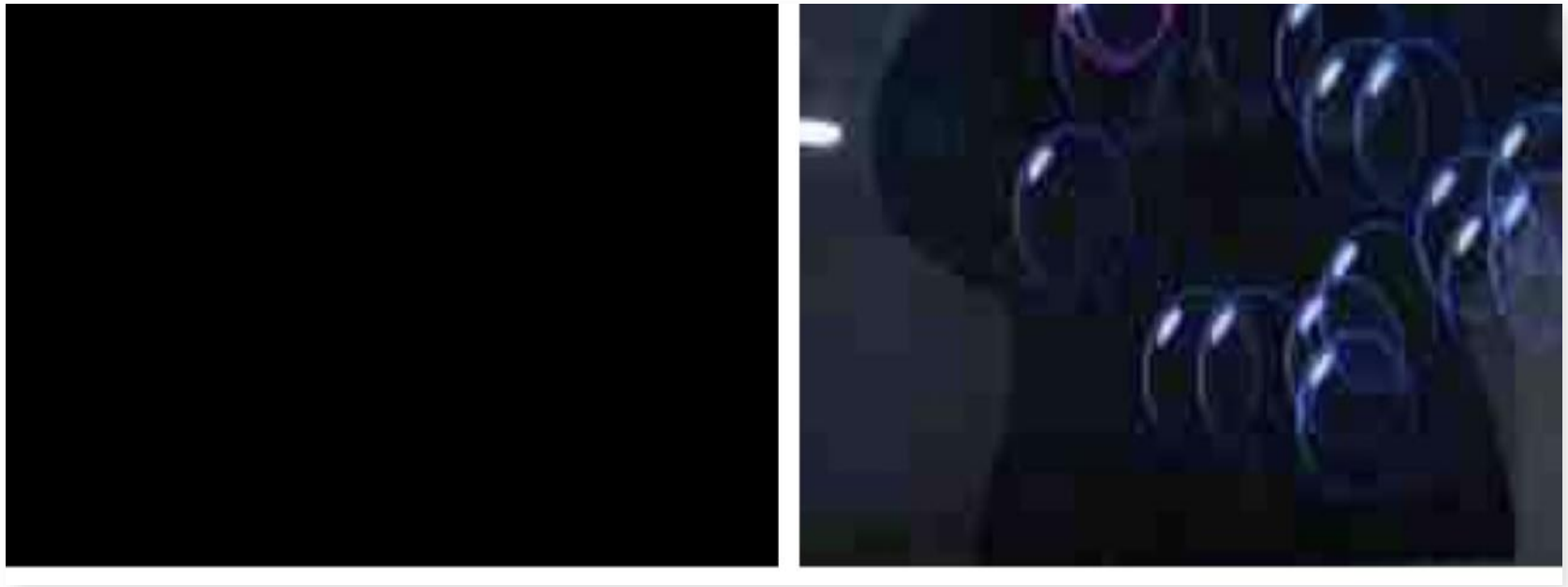
Air-Gap Exfiltration via High-Order Modulation-Based Screen Saver Covert Channels

Demonstration



Defense Techniques

- Screen savers still operate during idle time for privacy and display protection.
- They can be abused as covert visual channels in air-gapped systems.
- We counter this by degrading screen-saver image resolution to disrupt decoding.



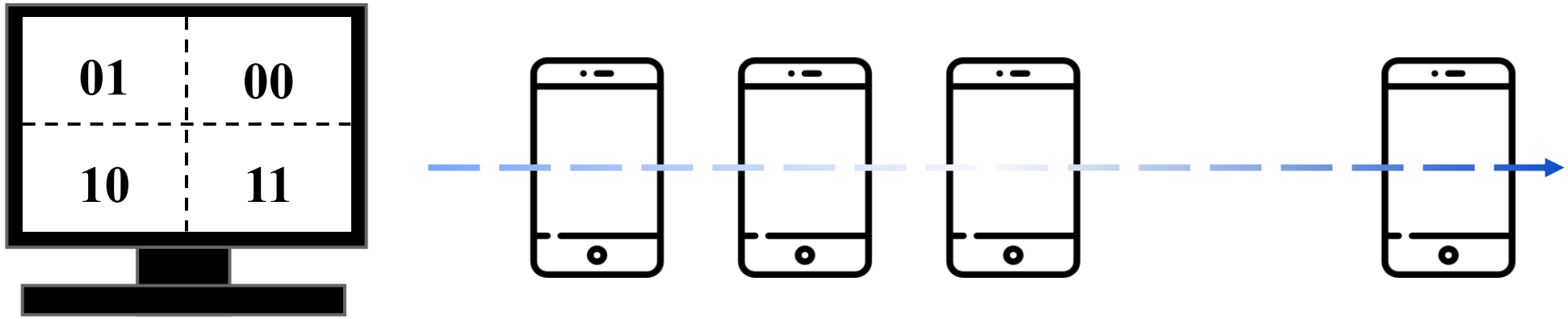
Evaluation

Environment

- ✓ Devices: Samsung Galaxy Book Pro, Galaxy S25
- ✓ Conventional: Exfiltrate via **QR codes** in images
- ✓ Proposed → implemented in Python

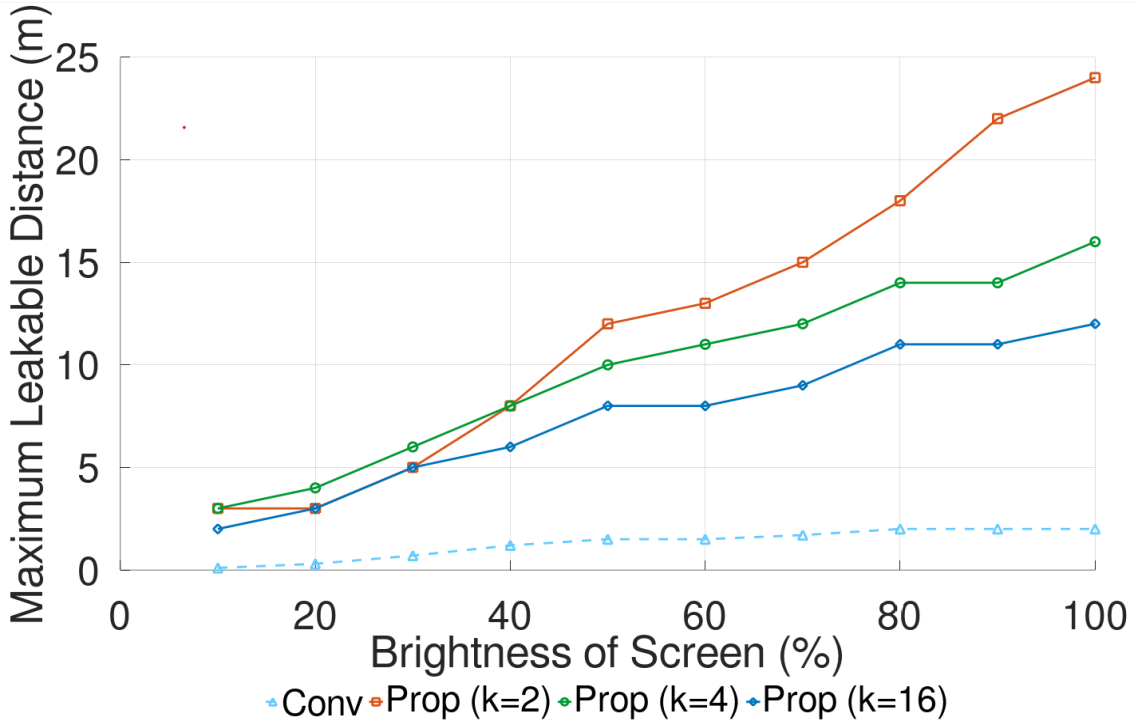
Setup

- ✓ Capture laptop screensaver with smartphone
- ✓ Gradually increase distance during capture
- ✓ Decode data using automated script



Evaluation

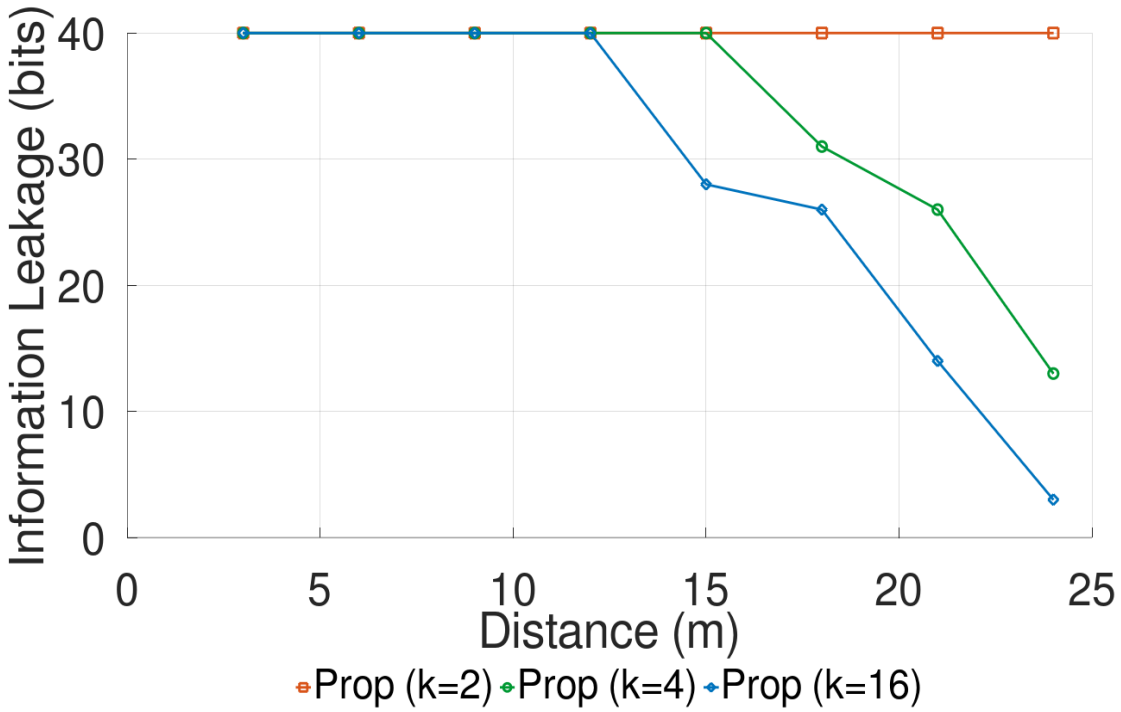
Leak Distance by Screen Brightness



- The conventional model embeds QR codes into images and the proposed model uses screensavers.
- ‘k’ represents the number of cells in the screensaver.
- Proposed method achieved the longest range, while QR code methods reached only 2 m.
- More cells = shorter distance, due to weaker visual clarity.
- QR-based recognition is **sensitive to lighting**, limiting reliability over distance.

Evaluation

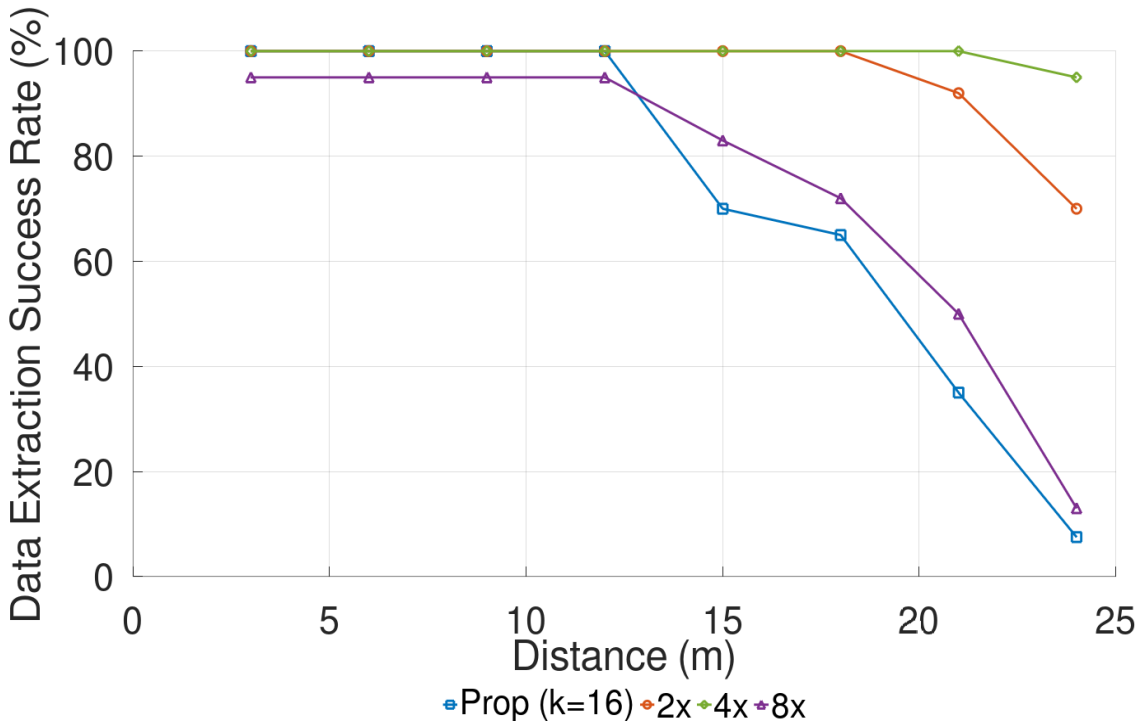
Information Extraction Success Rate by Cell Count



- The conventional model embeds QR codes into images and the proposed model uses screensavers.
- ‘k’ represents the number of cells in the screensaver.
- More cells reduce long-range reliability.
- **Fewer cells** improve stability but **limit data**.
- Larger screens balance both.

Evaluation

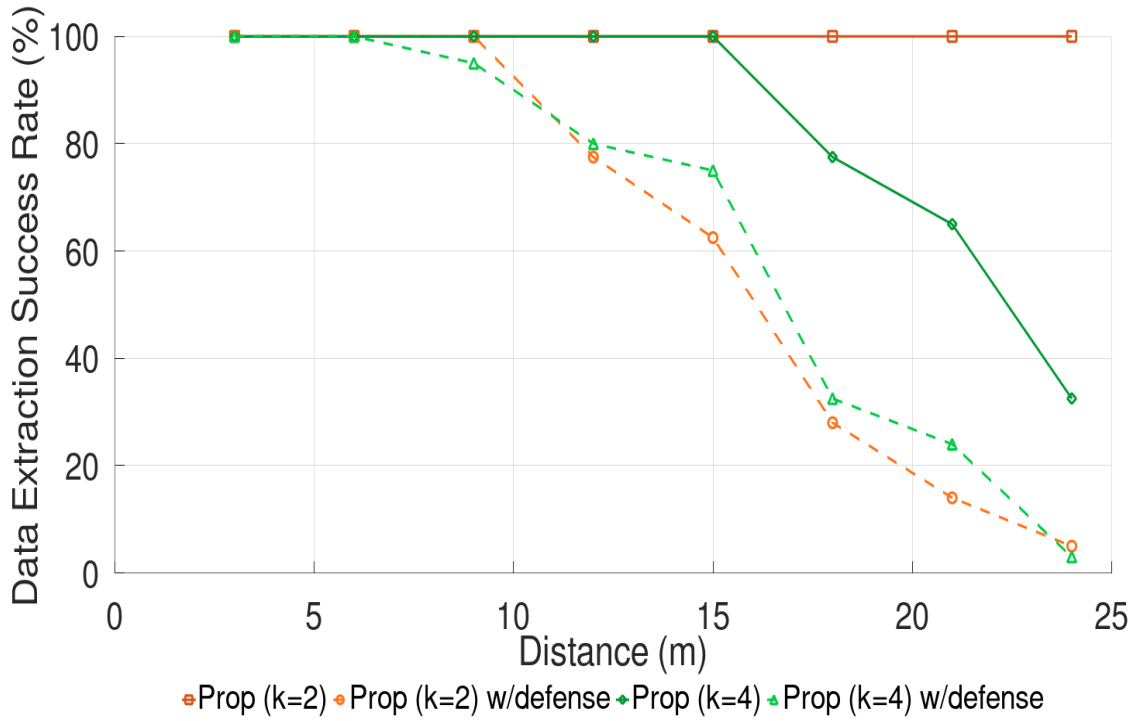
Data Extraction Success Rate vs Scaling Factor



- The conventional model embeds QR codes into images and the proposed model uses screensavers.
- ‘k’ represents the number of cells in the screensaver.
- The scaling factor refers to how many times the image quality has been enhanced using the AI-based correction program.
- **Proper image scaling** helps maintain clear cell boundaries and reduces noise interference during decoding.
- **Excessive scaling** amplifies visual noise and artifacts, ultimately lowering extraction accuracy.

Evaluation

Data Extraction Success Rate vs Image Quality



- The conventional model embeds QR codes into images and the proposed model uses screensavers.
- ‘k’ represents the number of cells in the screensaver.
- The proposed defense reduced decoding success by up to 95% (average ~30%)
- **Lower screensaver quality** leads to blurred cell boundaries, making extraction unreliable
- Controlling screensaver resolution can act as an **effective security layer in air-gapped systems**

Conclusion

- Summary

Attack model

Max exfiltration distance
~13x conventional

Proper scaling

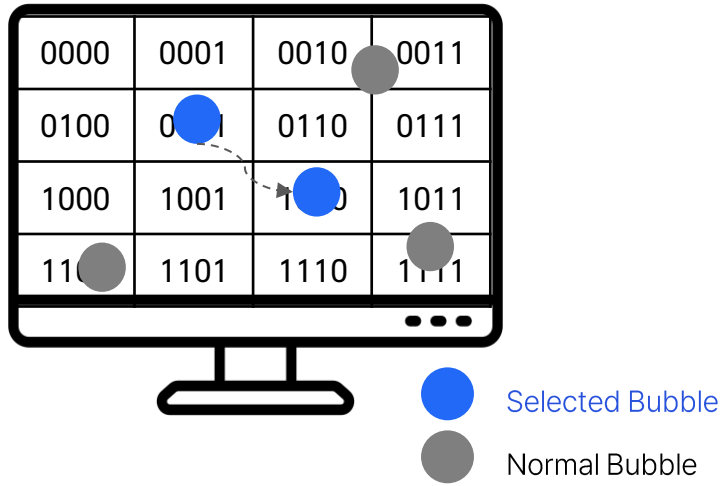
Extraction success rate ↑
up to 7.6x

With defense

Extraction success rate ↓
up to 95%

- Contributions
  - Novel data-leakage and defense techniques for air-gapped systems using screensavers
  - Attack feasibility tests confirmed the impact of cell size and cell count
  - Defense approach proven practical with experimental performance results

- Further Work
  - Comparative analysis of countermeasures for screensaver-based data exfiltration



Thank You !

Air-Gap Exfiltration via High-Order Modulation-Based Screen Saver Covert Channels

Sungshin Women's University
Ye-Rim Jeong | Yeon-Jin Kim | Chea-Yeon Park | Il-Gu Lee
220254016@sungshin.ac.kr