# CamShield: Securing Smart Cameras through Physical Replication and Isolation

Zhiwei Wang, Yihui Yan, Yueli Yan, Huangxun Chen*, **Zhice Yang**

ShanghaiTech University, *Huawei Theory Lab


上海科技大学
ShanghaiTech University

HUAWEI

# Visual Sensors are Ubiquitous

Smartphone

TV

Pet Monitor

Drone

Security Camera

Refrigerator

Vehicle

# News

## Google Disables Xiaomi Integration After Nest Hub Picks Up Random Camera Feed

A user's Google Nest Hub was showing images from a random camera feed instead of his own Xiaom smart IP security camera.

January 03, 2020 Steve Karantzoulidis Jump to Comments

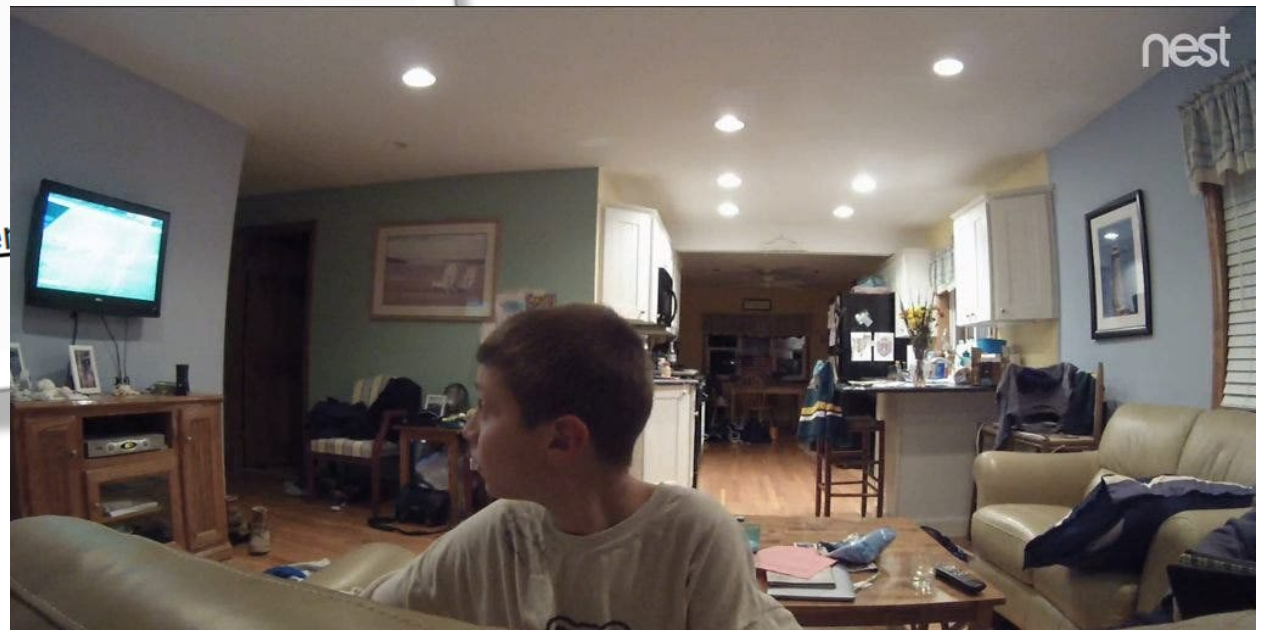

*(Source: securitysales.com)*

# More

## Buyer Beware: Used Nest Cams Can Let People Spy on You

**UPDATED JUNE 20, 2019**

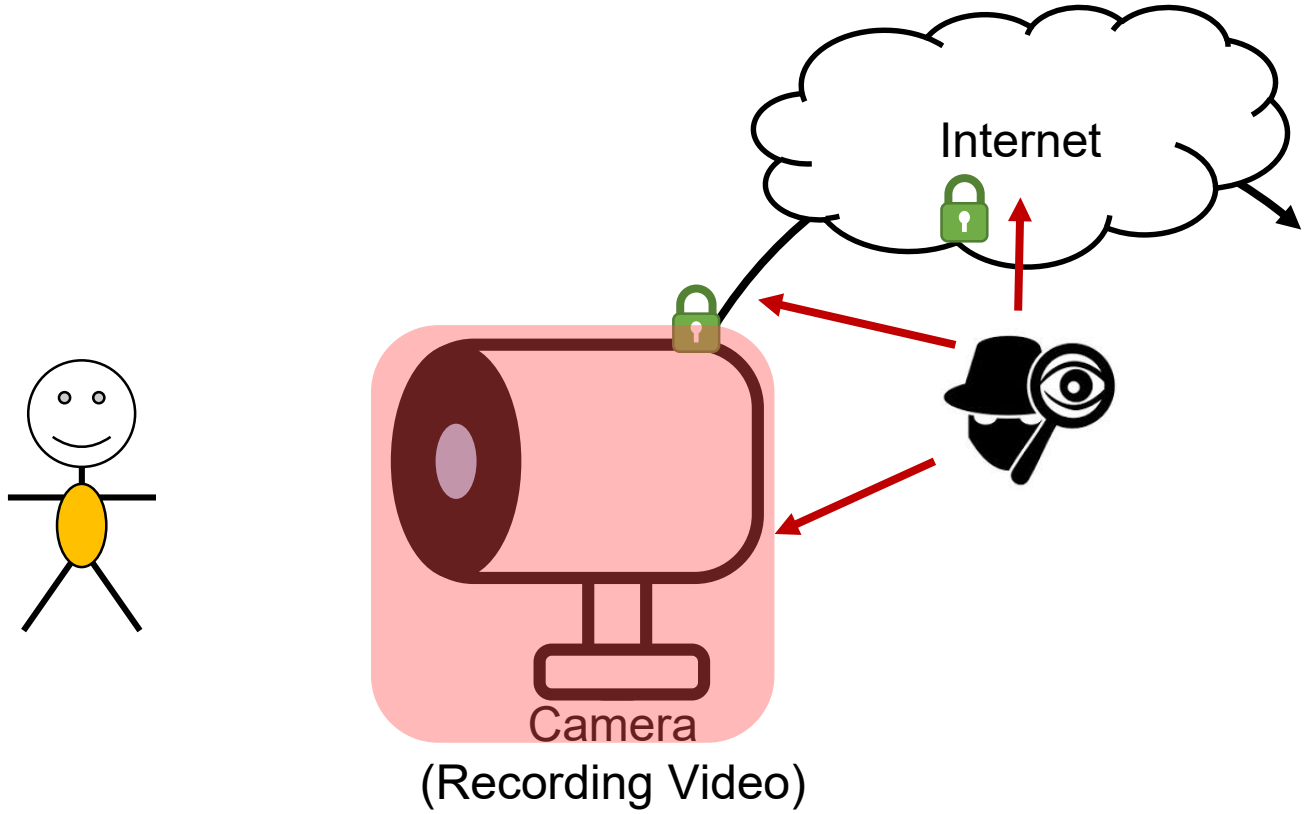
After our story broke yesterday, Google sent us a statemen
for the problem.



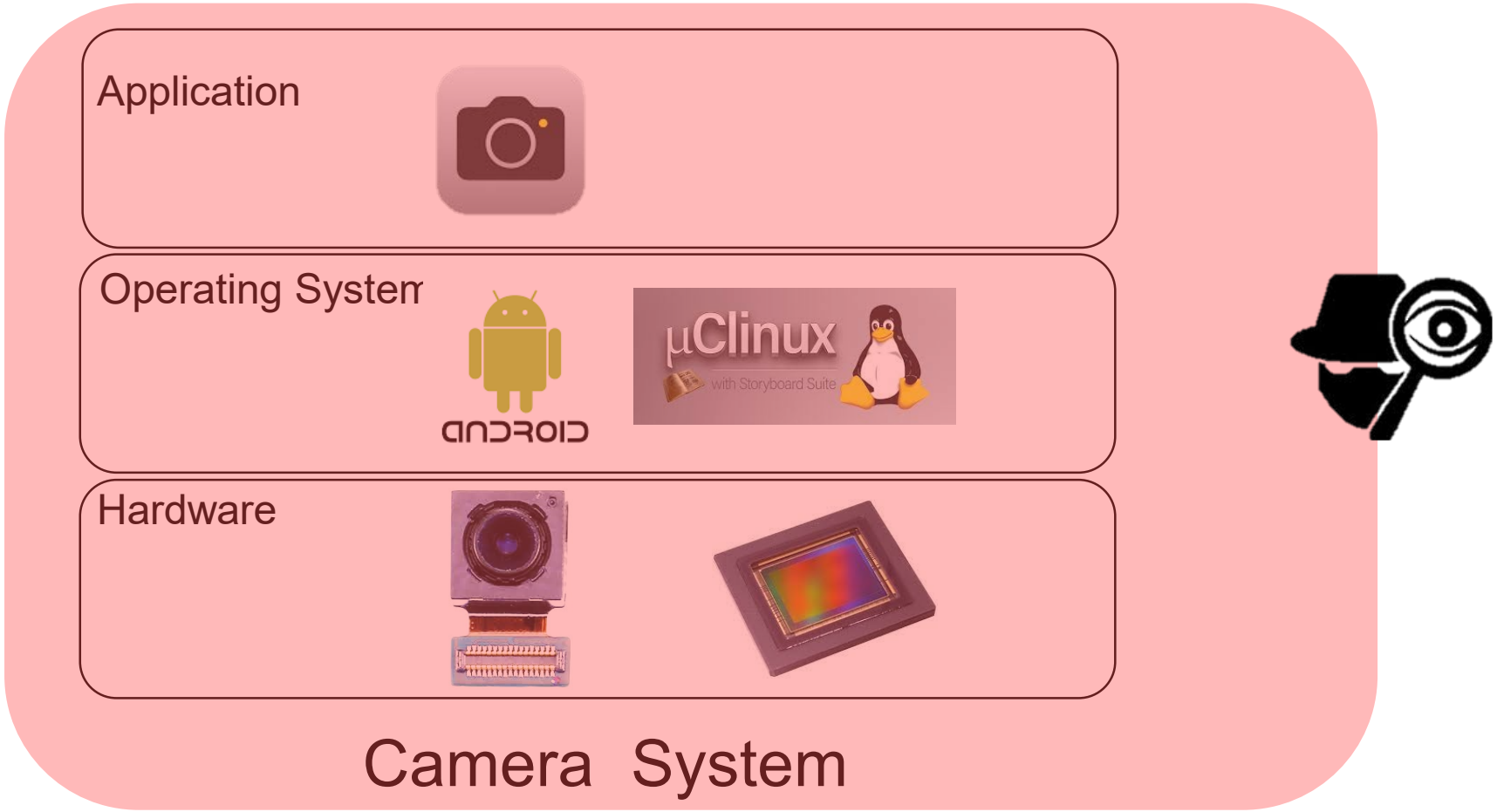

*(Source: nytimes.com)*

# Encryption alone is Insufficient

- We are not sure if the camera can be trusted (the prerequisite for encryption to take effect)



# Root of Trust



# Trust-nothing Solution

- Mark Zuckerberg Tapes over His Webcam. Should We?
  - Secure but block everything

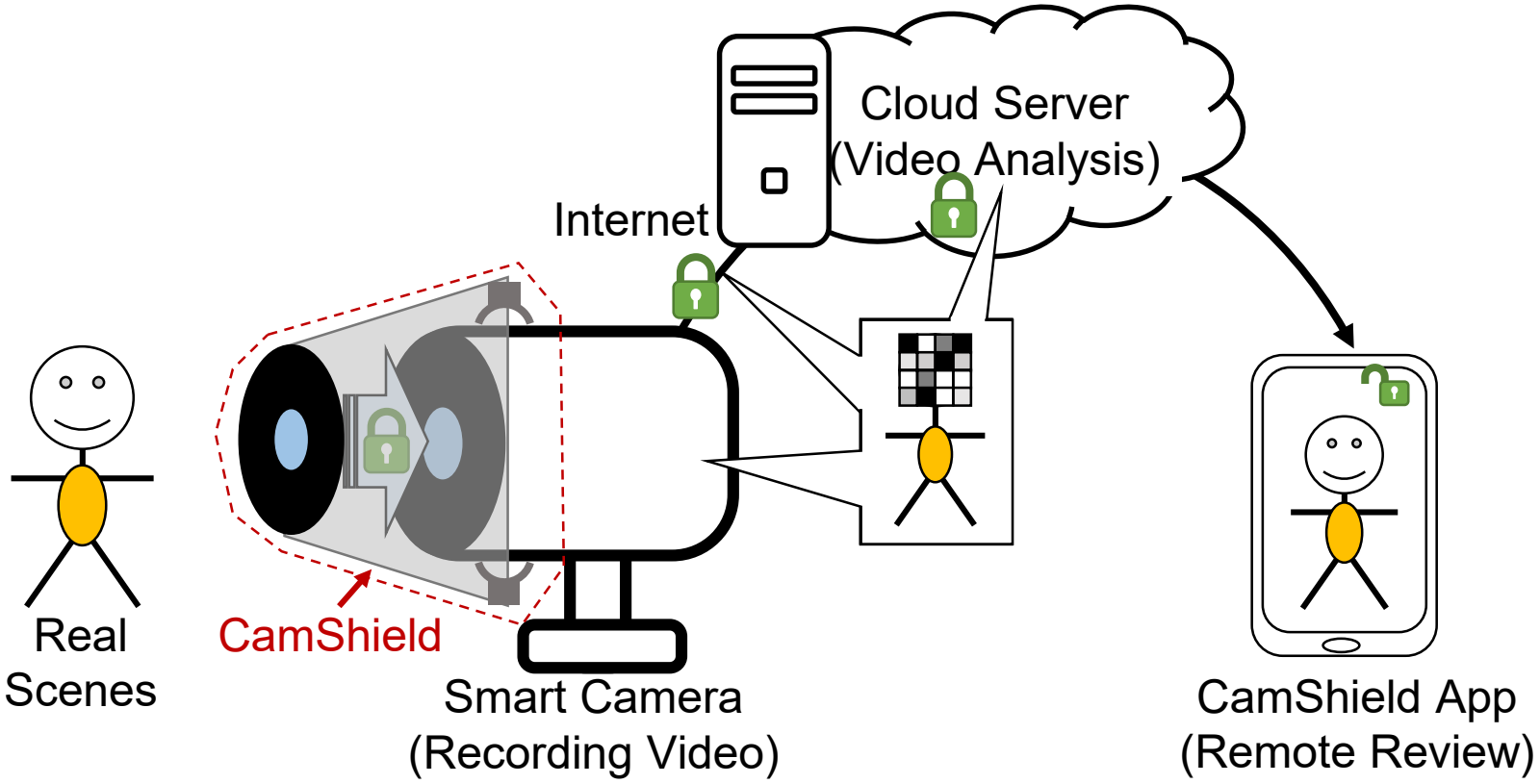

*(Source: theguardian.com)*

# CamShield – Bolt-on Root of Trust

1. Protect Visual Privacy and Retain Functionalities.

2. Compatible with Existing Cameras.

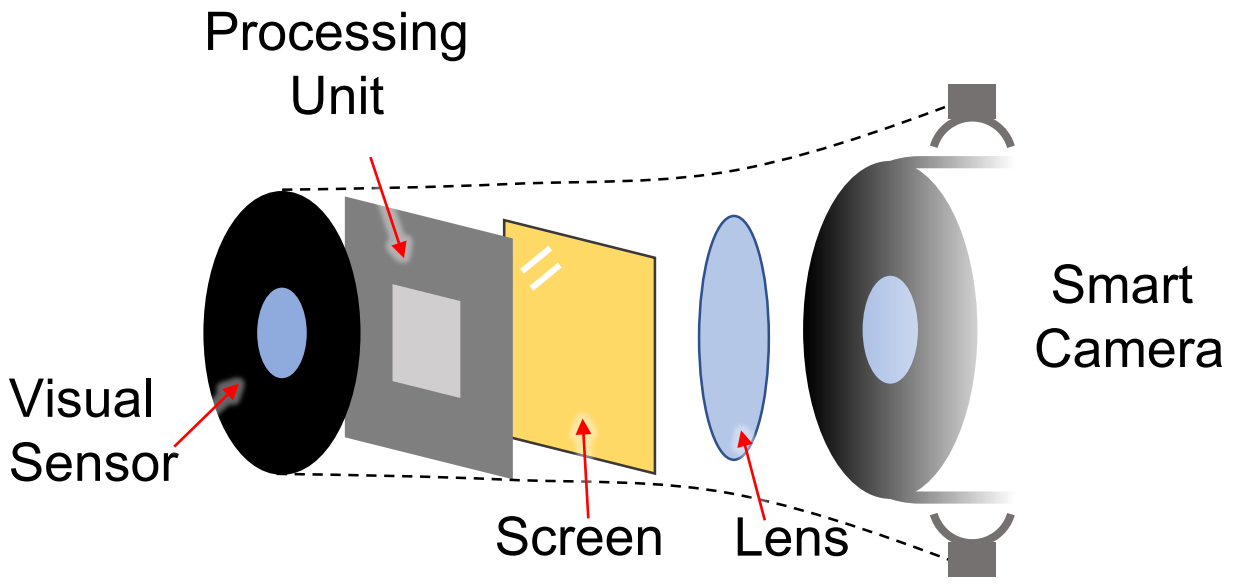
# CamShield – Approach



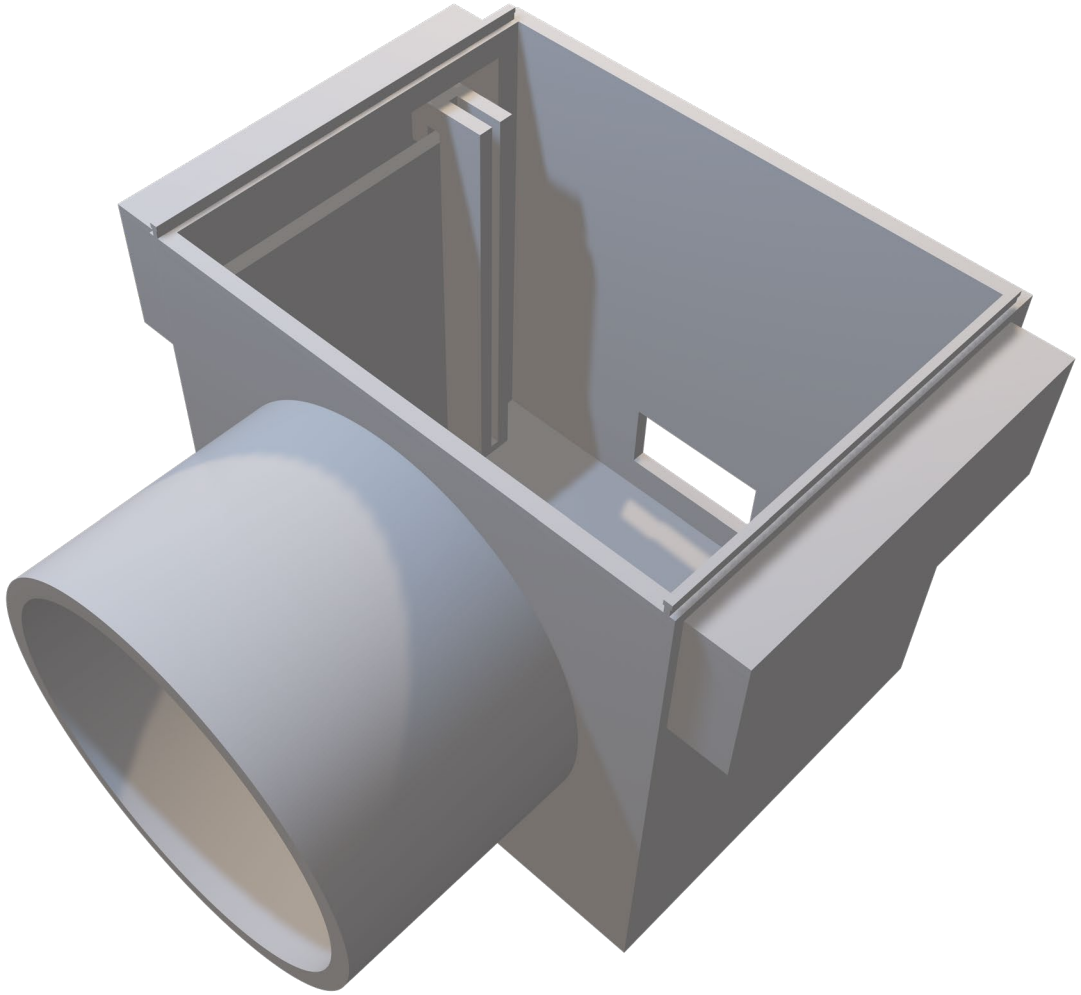
# CamShield – Approach

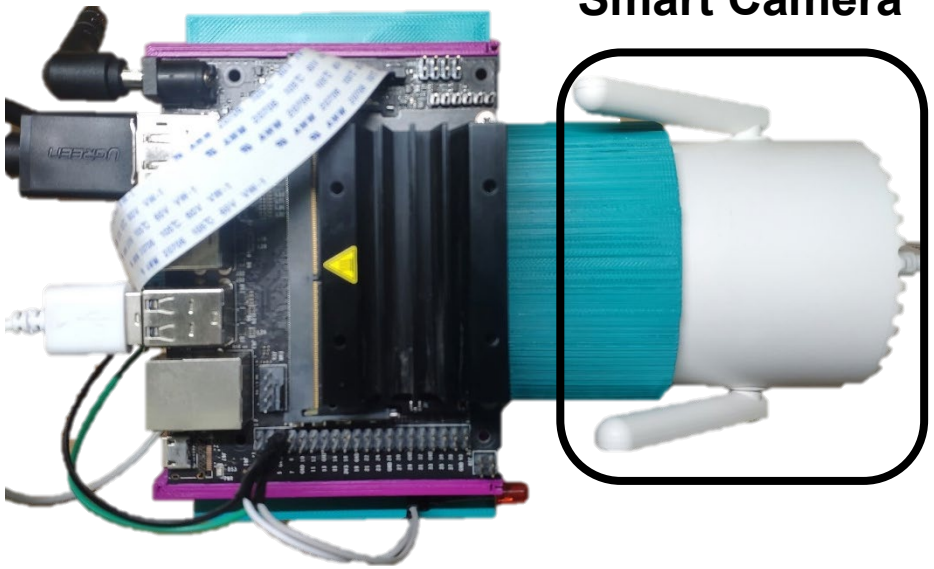
- Approach: **Physical Replication and Isolation**
- Why the protection is trustworthy?
  - ➢**Isolation**
- How does the protection affect original camera functionalities?
  - ➢**Replication**

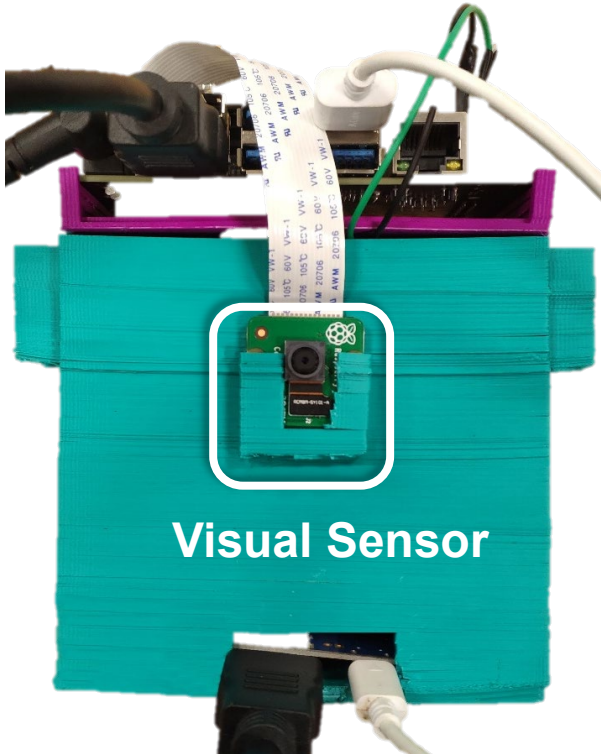
# CamShield Hardware



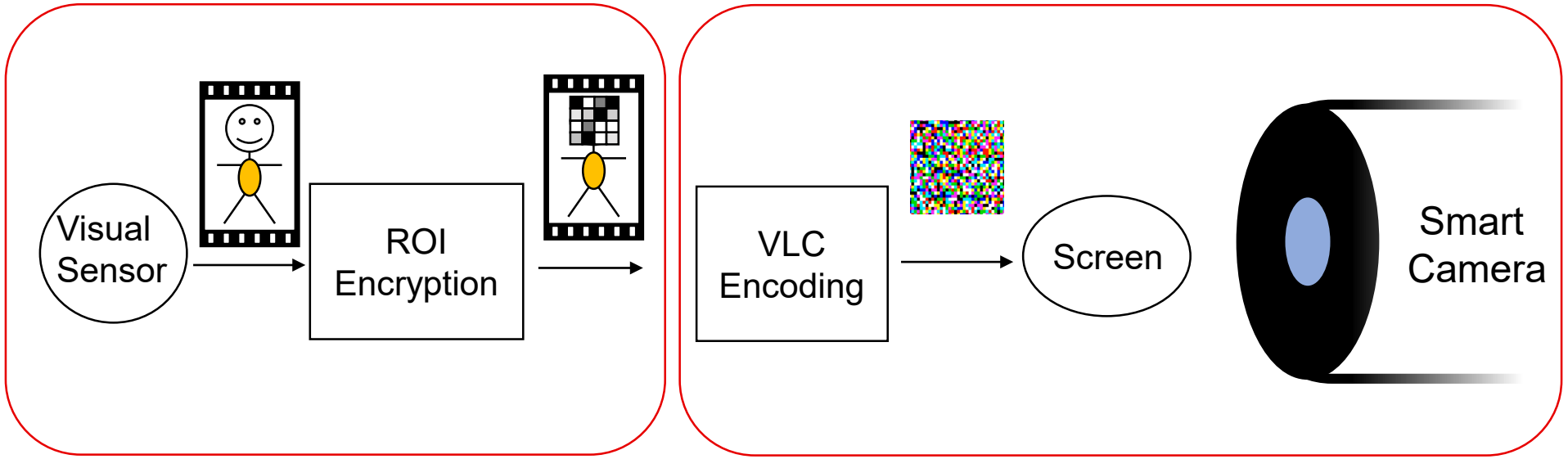
# Hardware Prototype





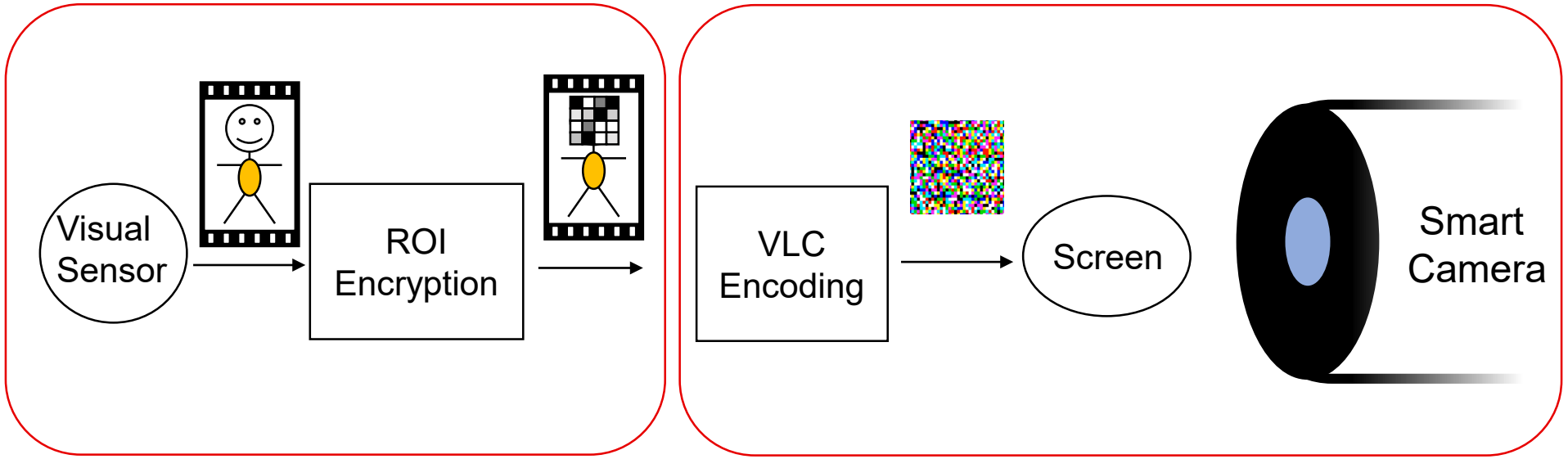



# CamShield Software




- Region of Interest (ROI) Encryption
- Visible Light Communication (VLC) Data Path

# CamShield Software



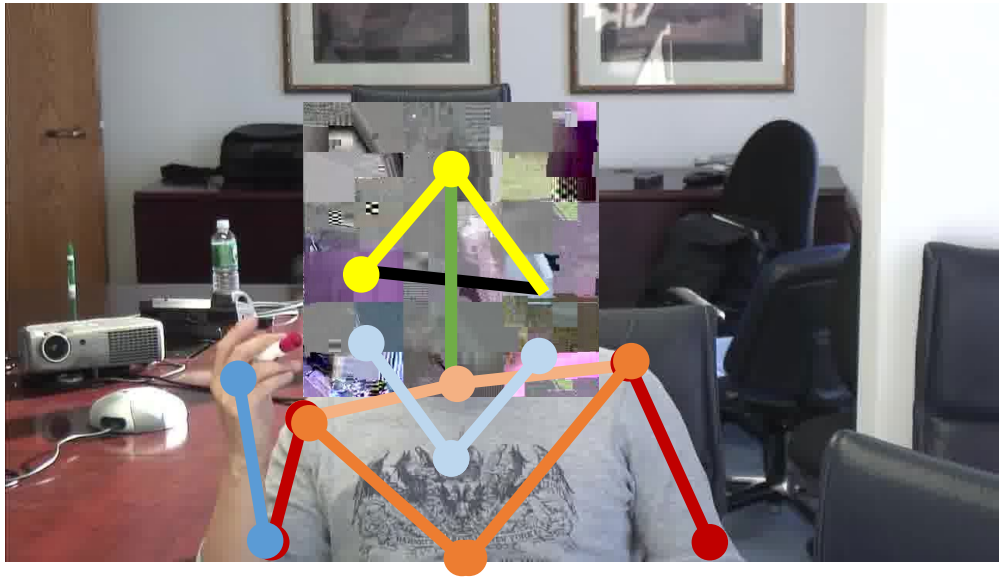

- Region of Interest (ROI) Encryption
- Visible Light Communication (VLC) Data Path

# Whole-frame v.s. Partial Encryption

- **Whole-frame Encryption**: full protection, disallows cloud analysis.
- **Partial Encryption**: the cloud server can still extract information, like motions or gestures, from the unencrypted parts.

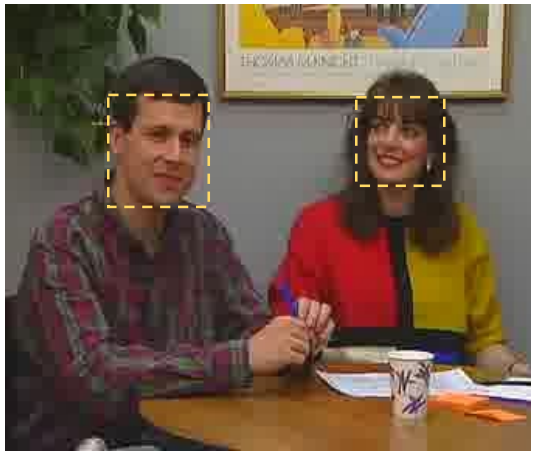
Whole Frame Encryption

V.S.



Partial Encryption

# ROI Encryption Workflow



① ROI Detection
(CV Algorithm)

② HEVC (H.265)
Encoding (Tile-based)

③ ROI Encryption

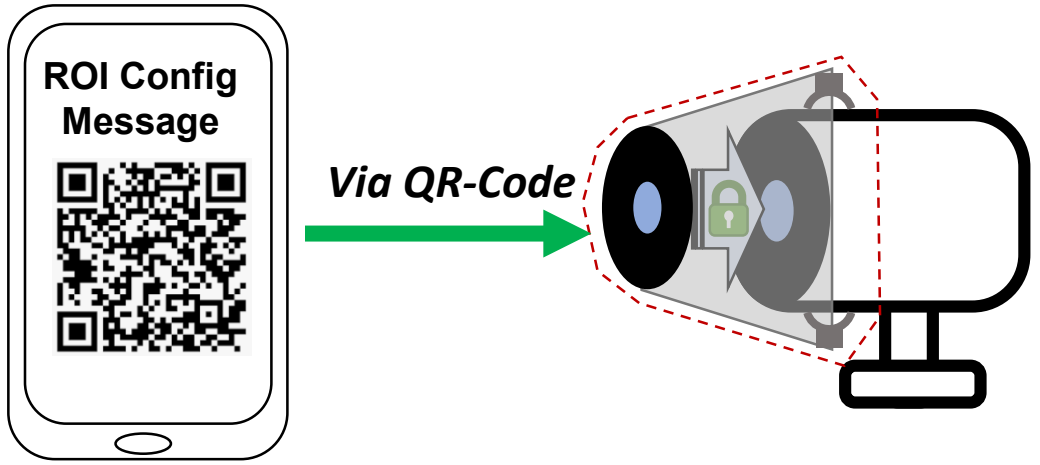
# ROI Configuration

- ROI Policies

| Index | ROI | Invert | Alg. | Time | Enable |
|---|---|---|---|---|---|
| 1 | all | F | / | all | F |
| 2 | none | F | / | all | F |
| 3 | face | F | mobile net | all | T |
| 4 | body | F | opencv | all | F |
| 5 | text | F | opencv | work days | F |

Table of ROI Entries

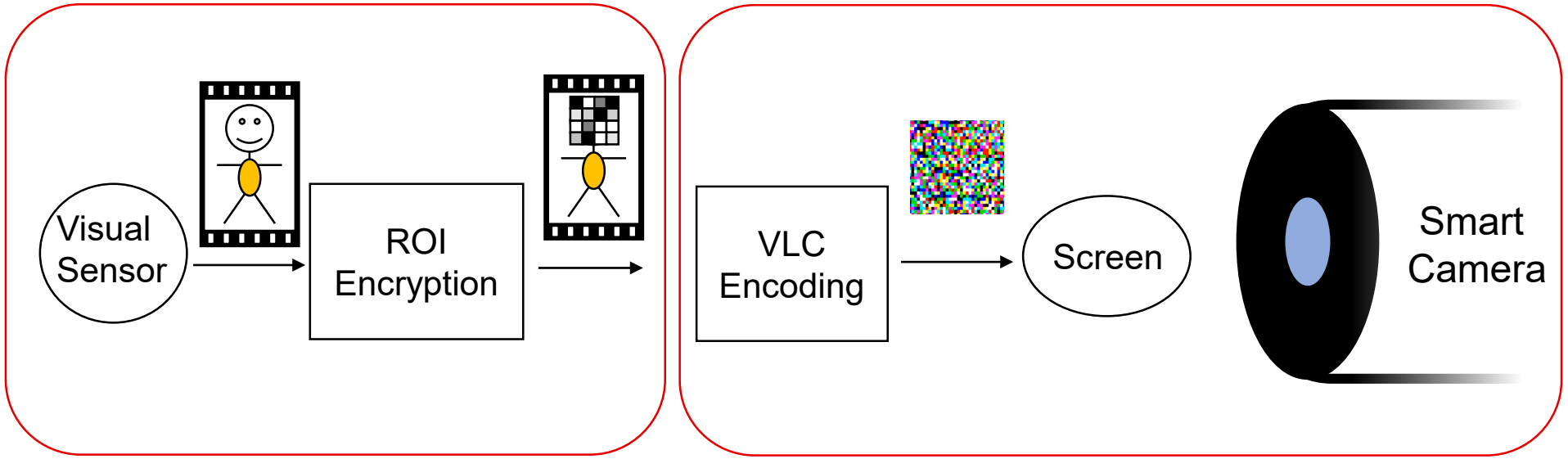
- Configuration Interface




CamShield App

CamShield Device

# CamShield Software

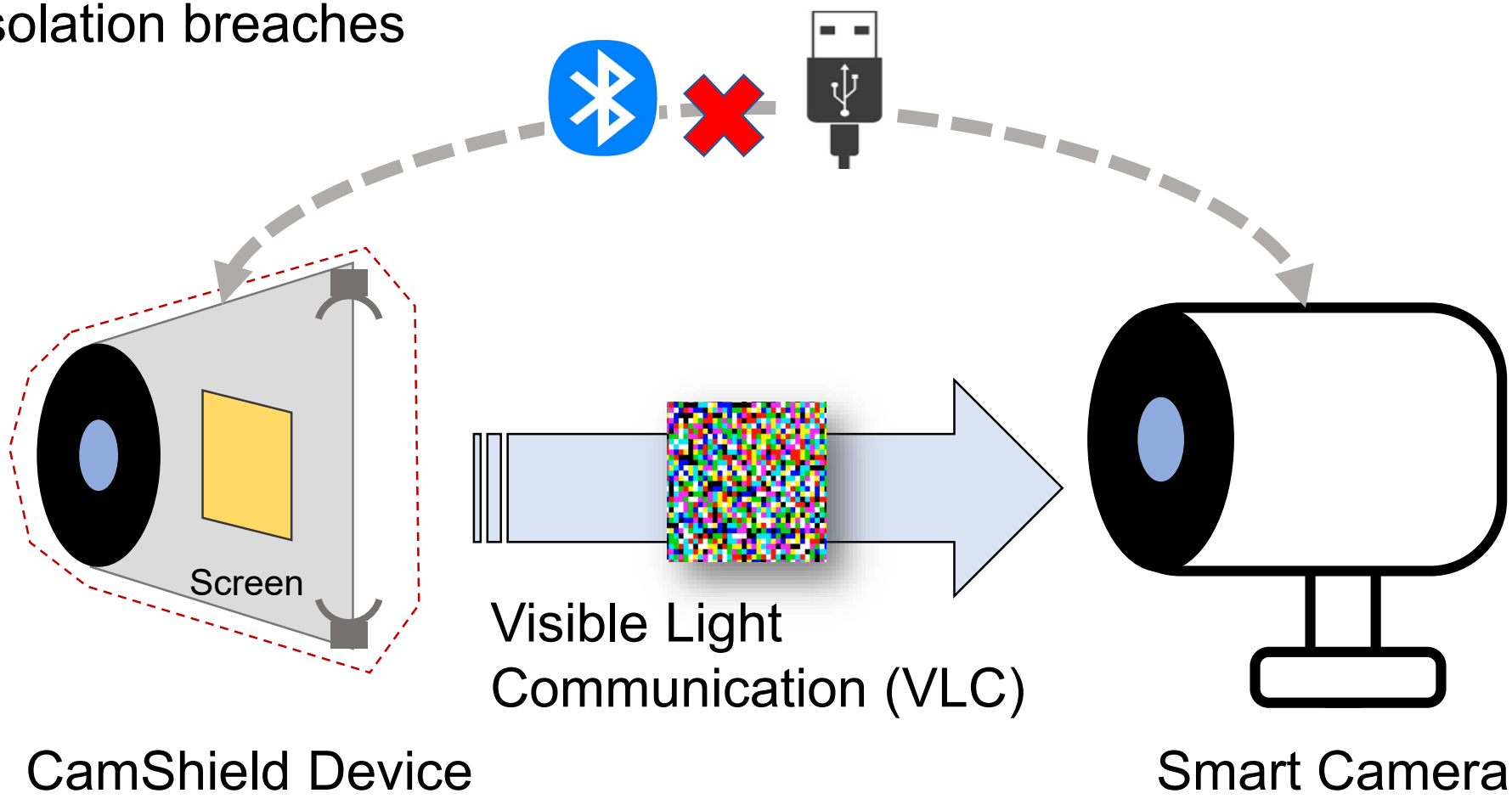



➢Region of Interest (ROI) Encryption

➢Visible Light Communication (VLC) Data Path

# How to Transfer Encrypted Video ?

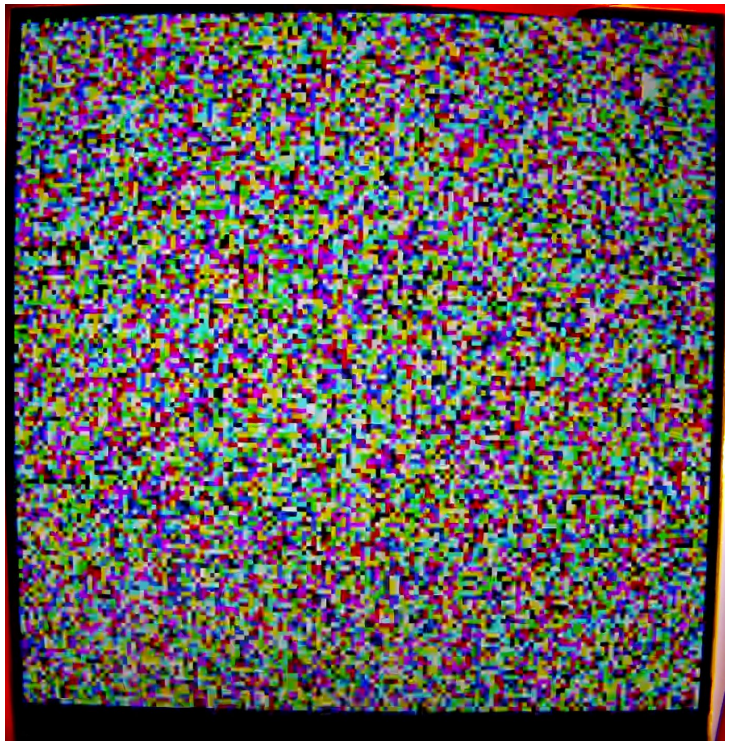
- Risks
  - Isolation breaches



# Visible Light Communication (VLC)

| Bits | Block Color |
|---|---|
| 000 | |
| 001 | |
| 010 | |
| 011 | |
| 100 | |
| 101 | |
| 110 | |
| 111 | |

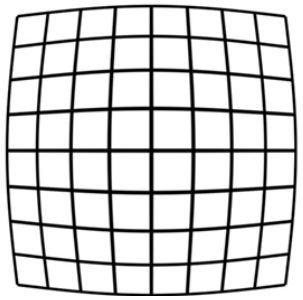
display content on the screen

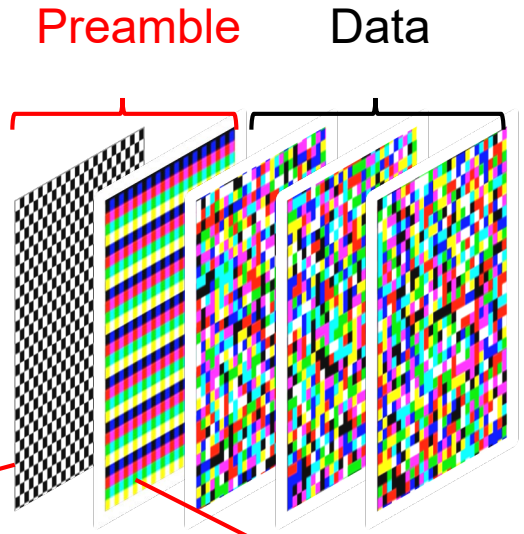


captured by the smart camera

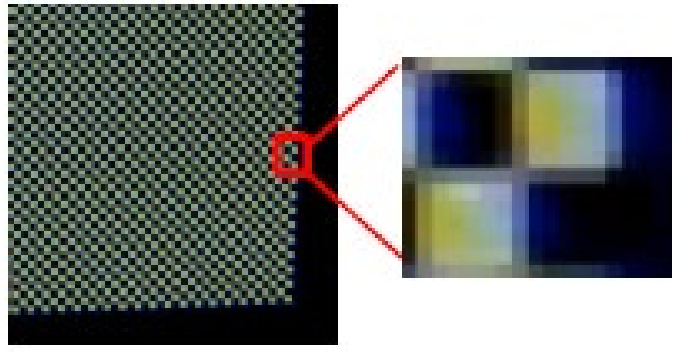
# Decoding VLC Streams

- Lens Distortion

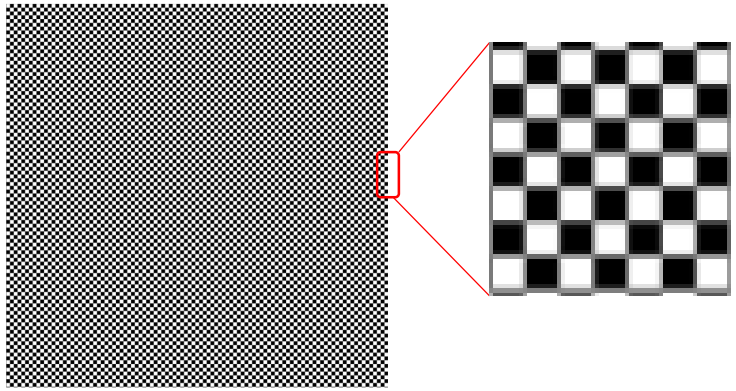




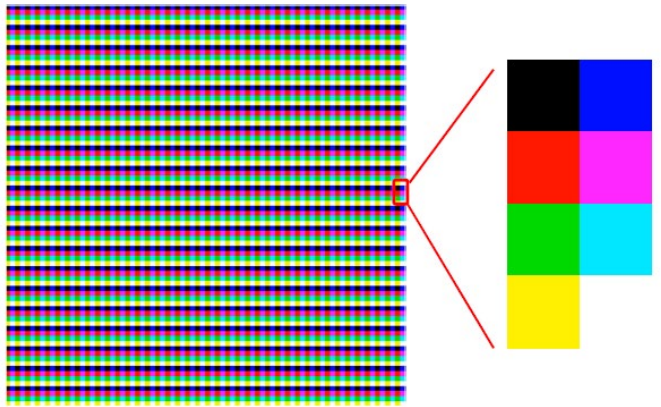

- Chromatic Distortion

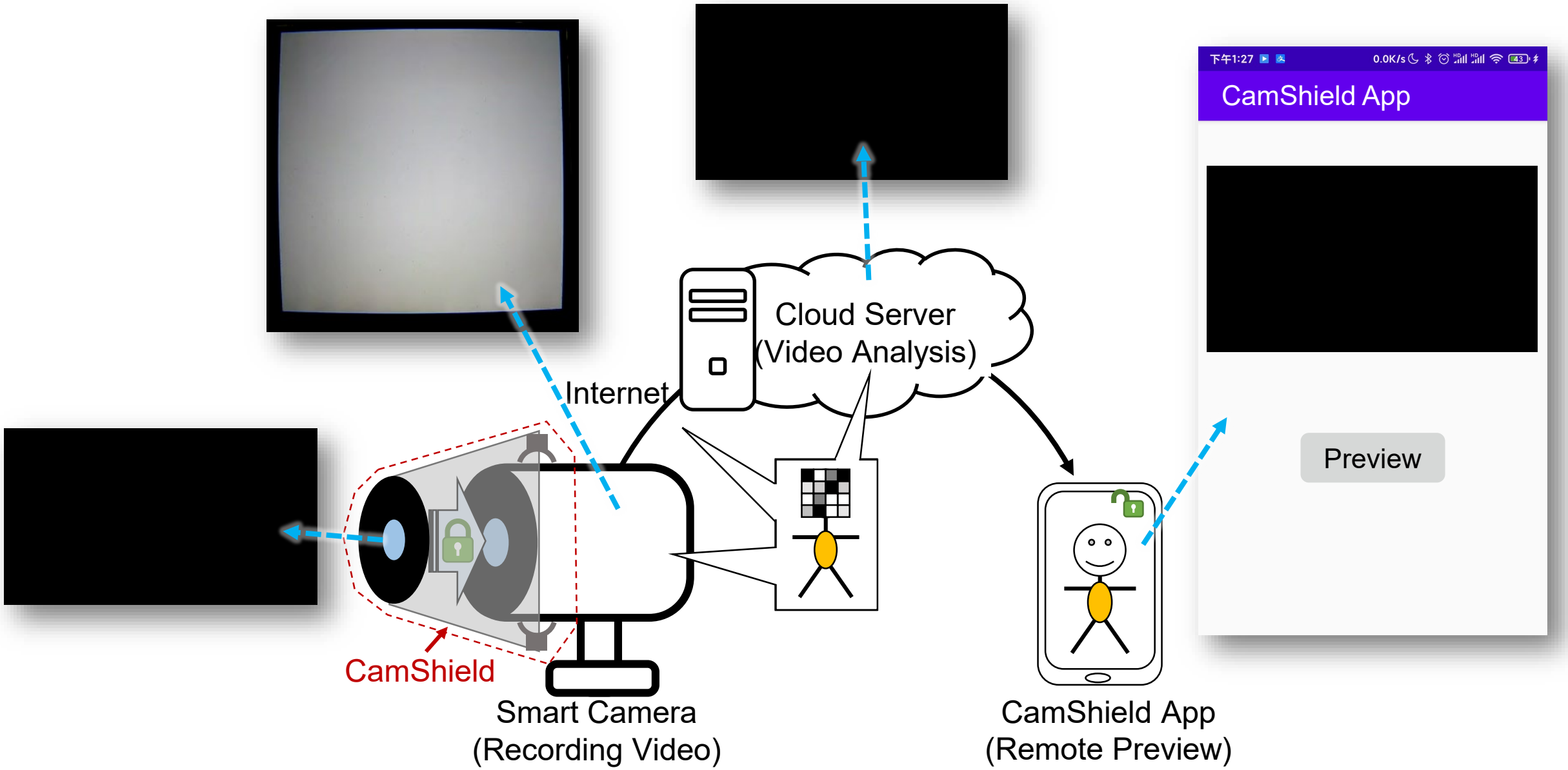


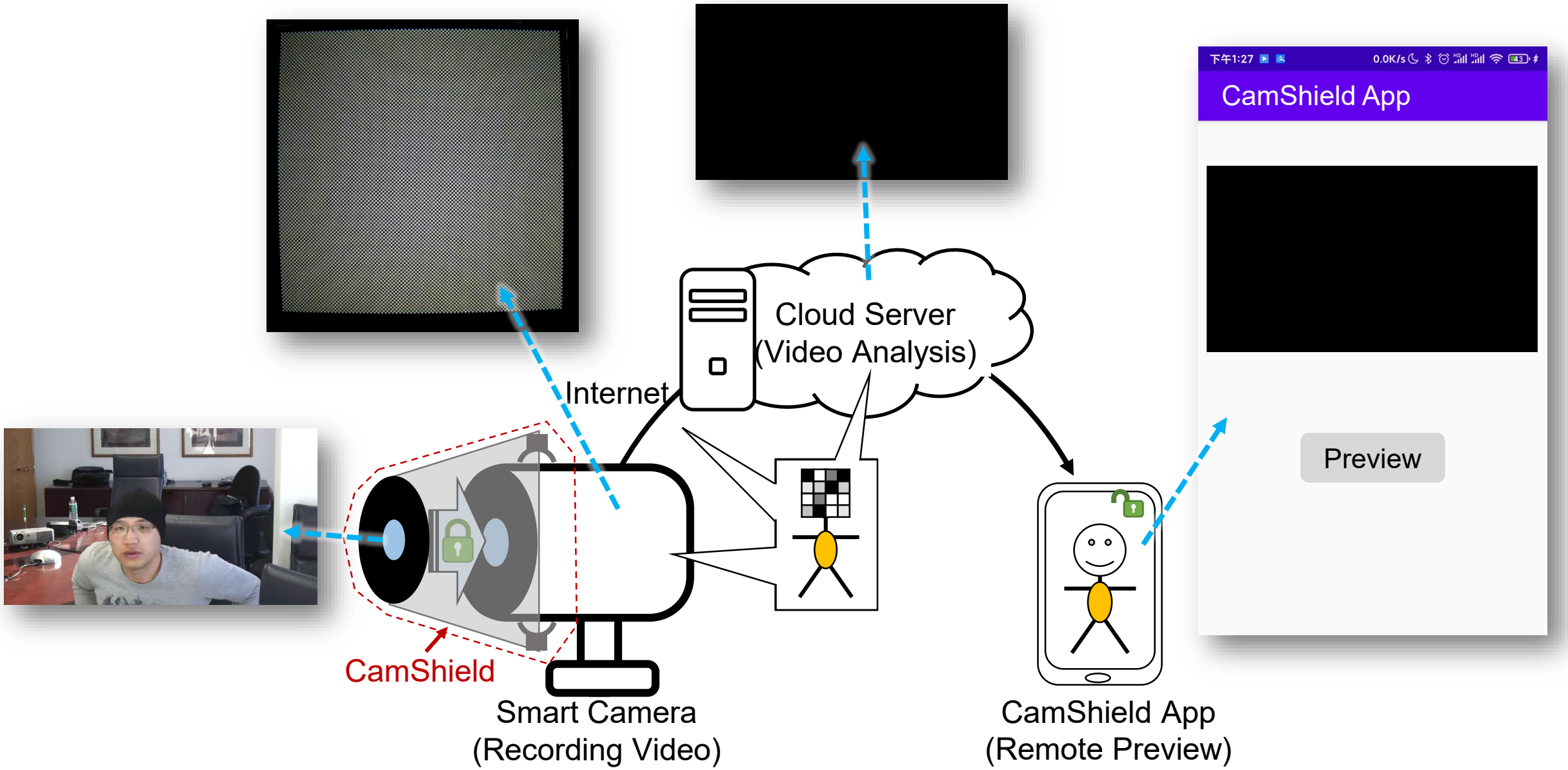
Grid Preamble

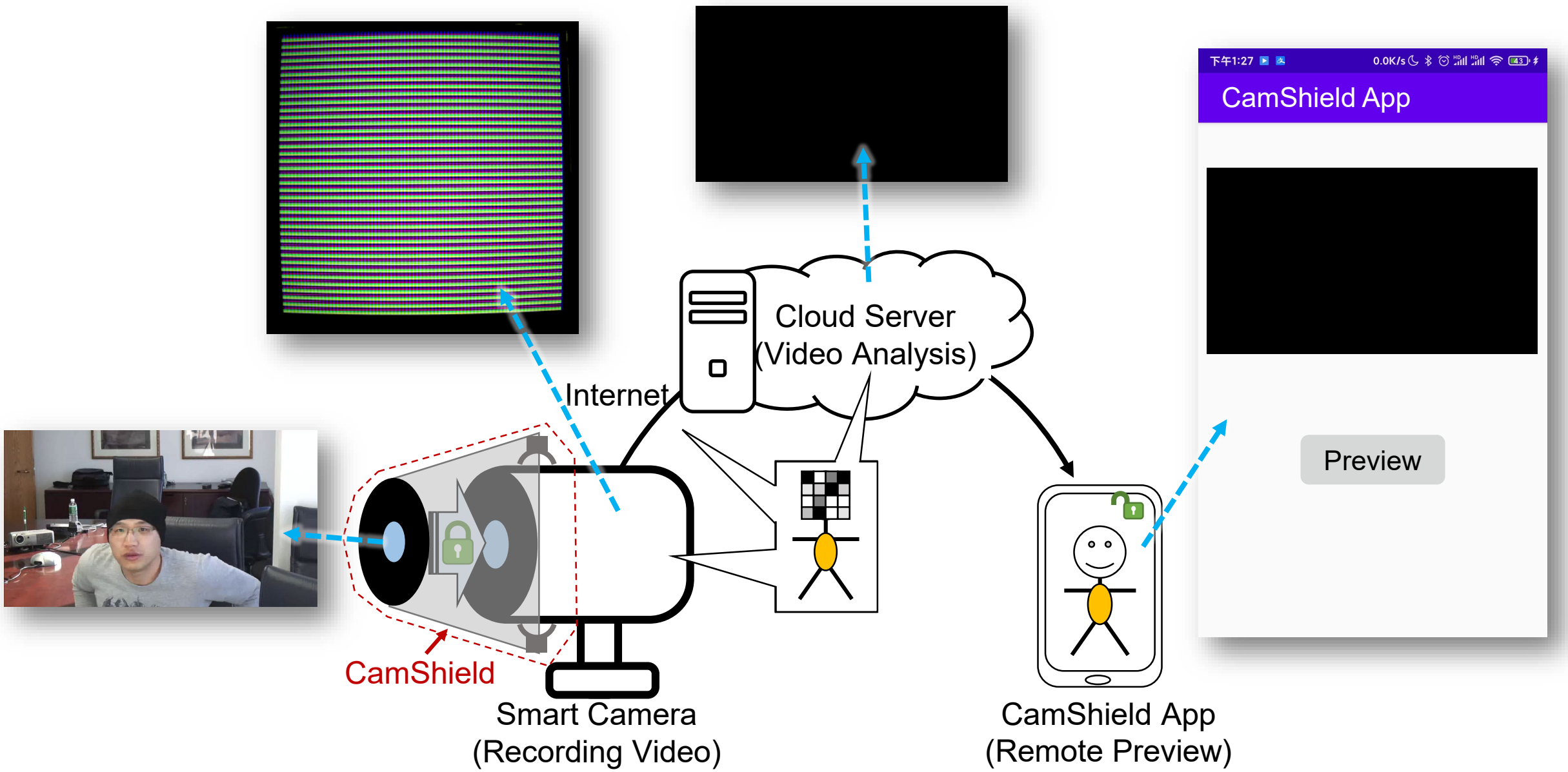


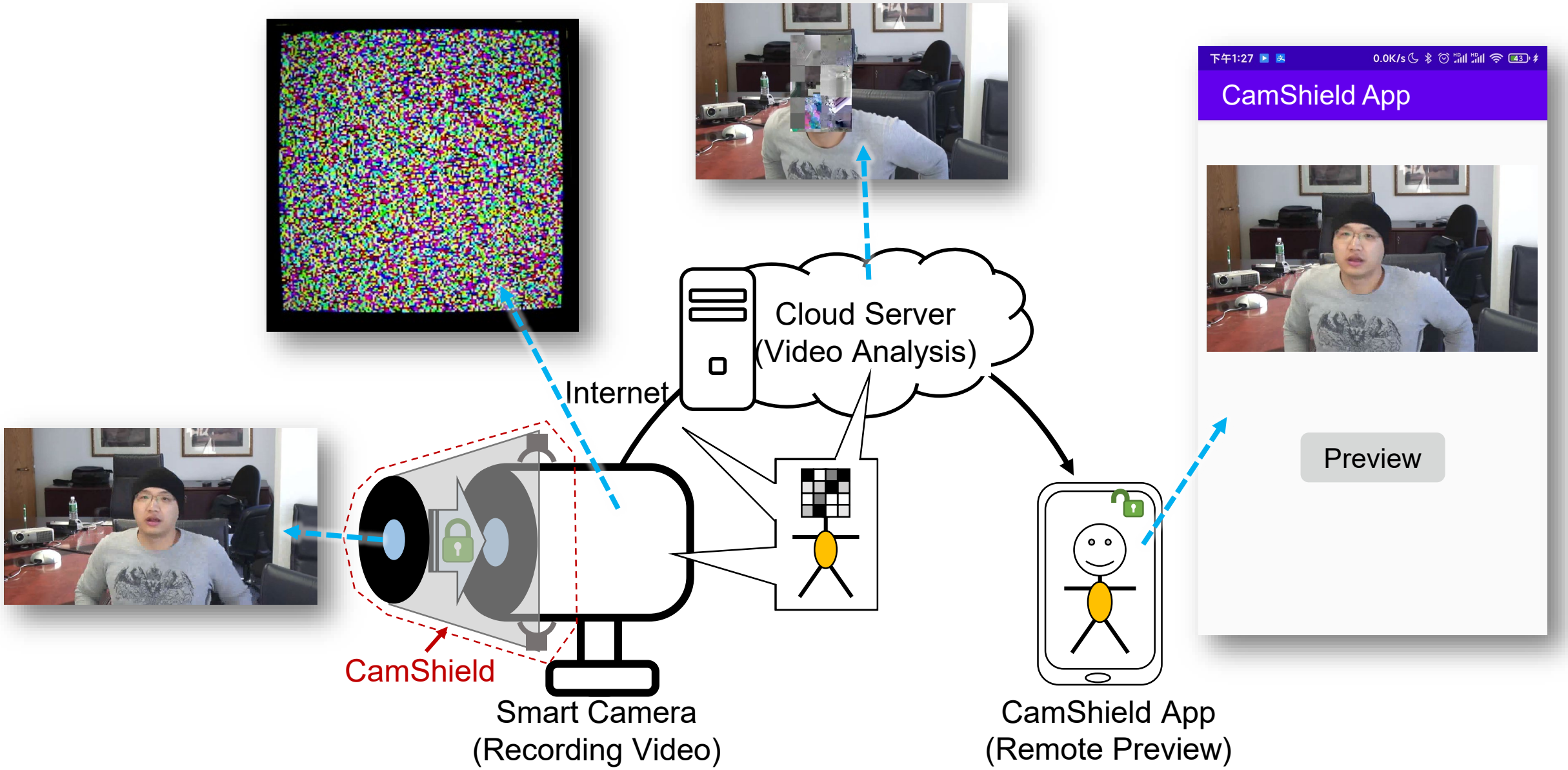
Color Palette Preamble




Cloud Server
(Video Analysis)
Internet
CamShield
Smart Camera
(Recording Video)
CamShield App
(Remote Preview)
下午1:27
0.0K/s
CamShield App
Preview


Cloud Server
(Video Analysis)
Internet
CamShield
Smart Camera
(Recording Video)
CamShield App
(Remote Preview)
下午1:27
0.0K/s
CamShield App
Preview


Cloud Server
(Video Analysis)
Internet
CamShield
Smart Camera
(Recording Video)
CamShield App
(Remote Preview)
下午1:27
0.0K/s
CamShield App
Preview


Cloud Server
(Video Analysis)
Internet
CamShield
Smart Camera
(Recording Video)
CamShield App
(Remote Preview)
下午1:27
0.0K/s
CamShield App
Preview

# Conclusion

- We propose an approach to secure visual sensing devices.

- Advantages
  - Bolt-on Solution: it is compatible with commercial cameras, and retains their functionalities.
  - Strong Protection: the shield device is not only logically but also physically isolated from the camera and the network, preventing it from many practical attacks.

# Thank You !

Contact: Zhice Yang yangzhc@shanghaitech.edu.cn