Do Not Share!
Invisible Light Beacons for Signaling Preferences to Privacy-Respecting Cameras

Ashwin Ashok

Viet Nguyen

Marco Gruteser

Narayan Mandayam

Wenjia Yuan

Kristin Dana

Our current life…

Wink with your right eye.

Can we keep privacy anymore?

Current solutions...

Preserving privacy for users/objects

Online photo sharing services: delete, untag, no publication...

People can control their taken photos online
After-the-fact

Store user privacy pref. on cloud servers

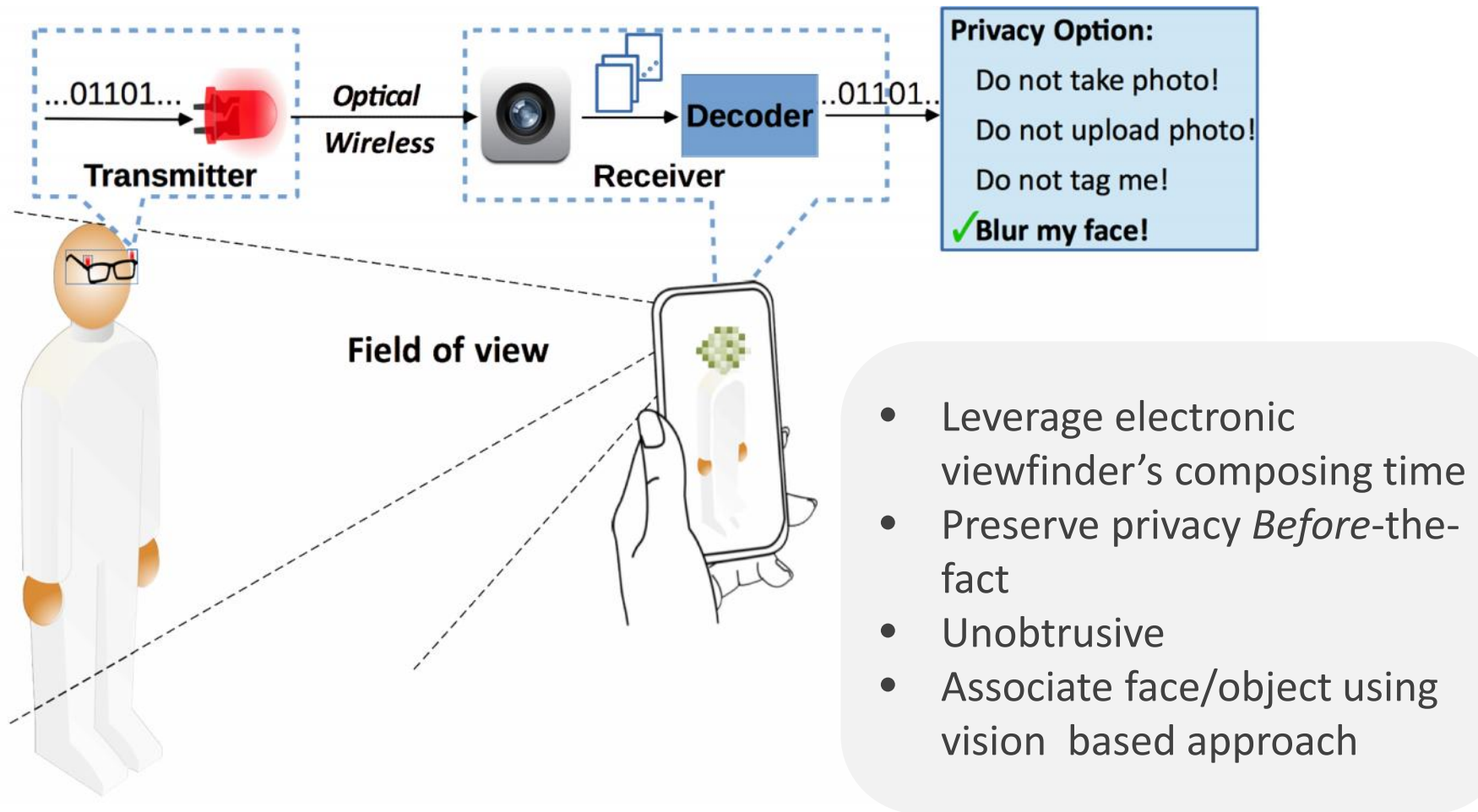People can specify privacy preference beforehand
Requires network connection

Physical notification

Remind users before taking photos
User behavior cannot be controlled

For copyright reasons, we cannot allow photos to be taken of single pieces of artwork.

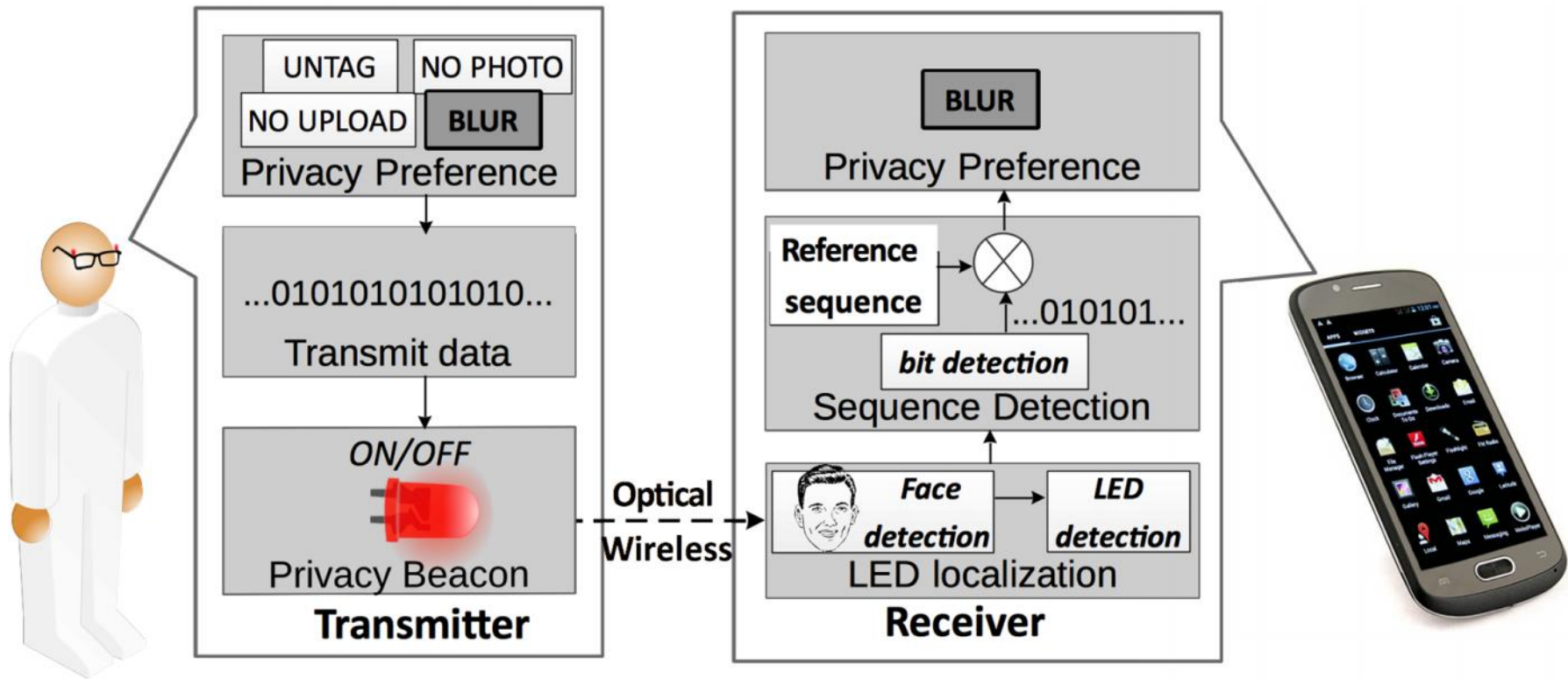You may, however, take general views of the galleries.

Are cameras intelligent enough to know
the privacy preference of the photographed entity?

Privacy-respecting cameras using (In)visible Light Communication

...01101... → **Optical Wireless** → ...01101... **Decoder** → ..01101..

Transmitter   **Receiver**

Privacy Option:
Do not take photo!
Do not upload photo!
Do not tag me!
✓ **Blur my face!**

Field of view

- Leverage electronic viewfinder's composing time
- Preserve privacy *Before*-the-fact
- Unobtrusive
- Associate face/object using vision based approach

System diagram

Evaluation

- What is the time available between application starts and user snaps photo (***composing time***)?

- What is the accuracy of detecting ***a universally agreed sequence of bits*** within the composing time?

- What is the probability of error for communicating ***a random stream of bits*** from the IR LED to an off-the-shelf camera device?
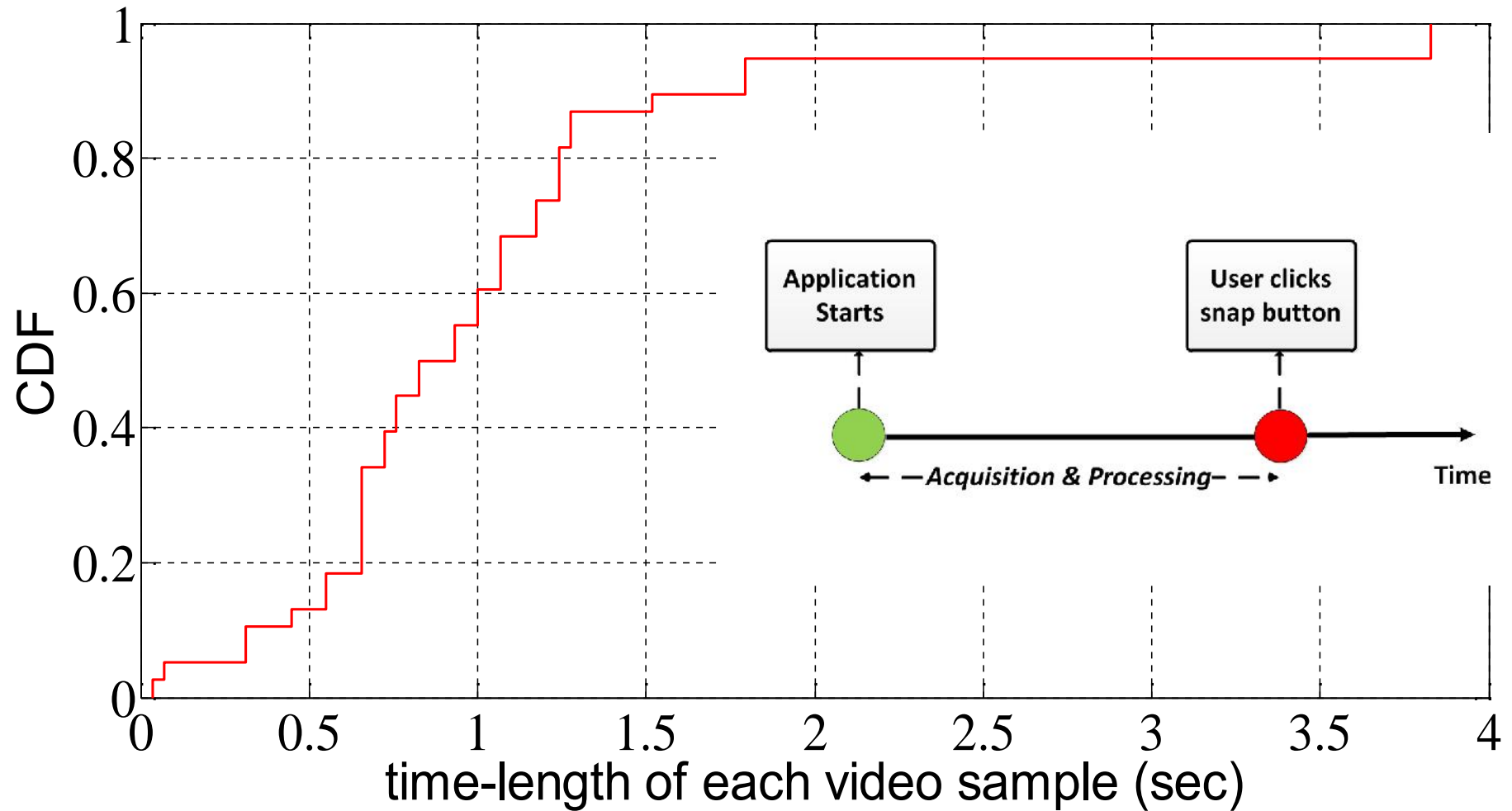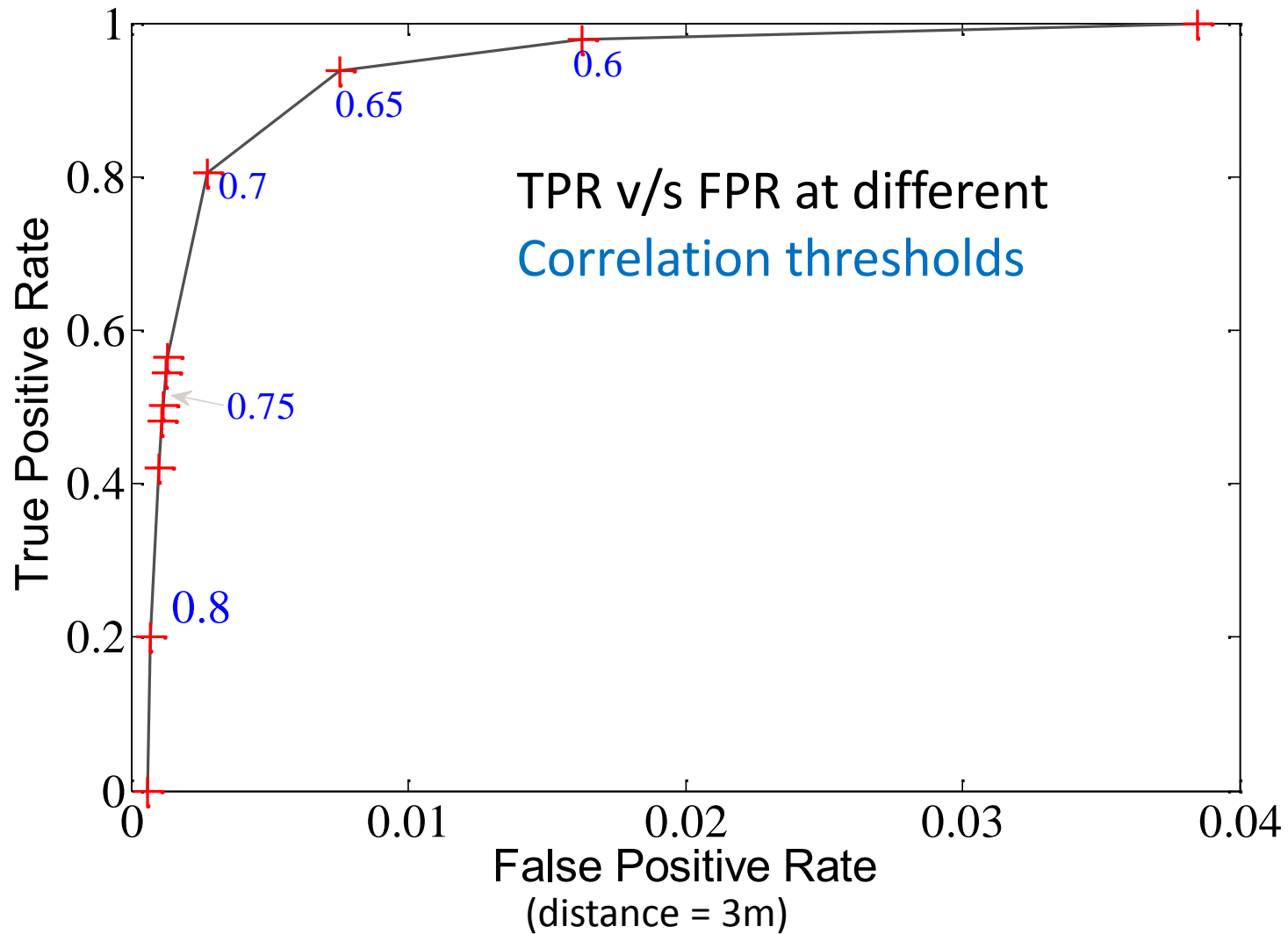
Experiment 1 : Barker sequence

- Samsung S2 smartphone, 30fps, 720x1080 resolution
- The video samples are processed on PC by OpenCV code (C++), using Viola-Jones object detection framework
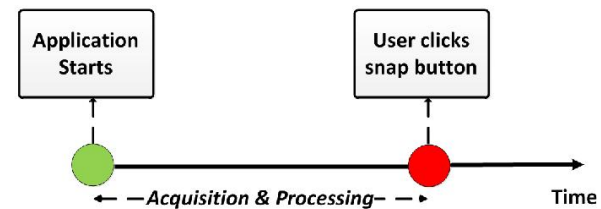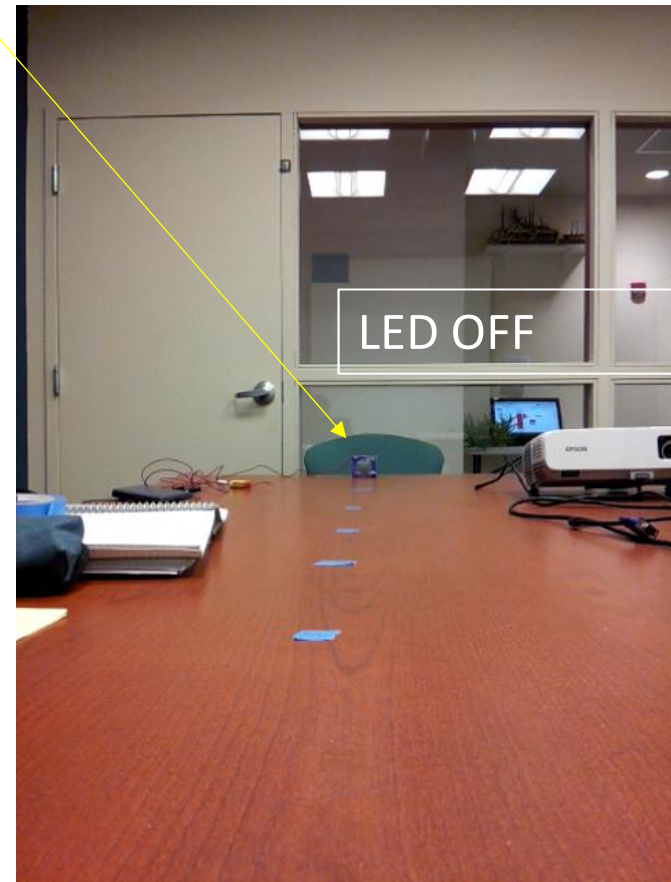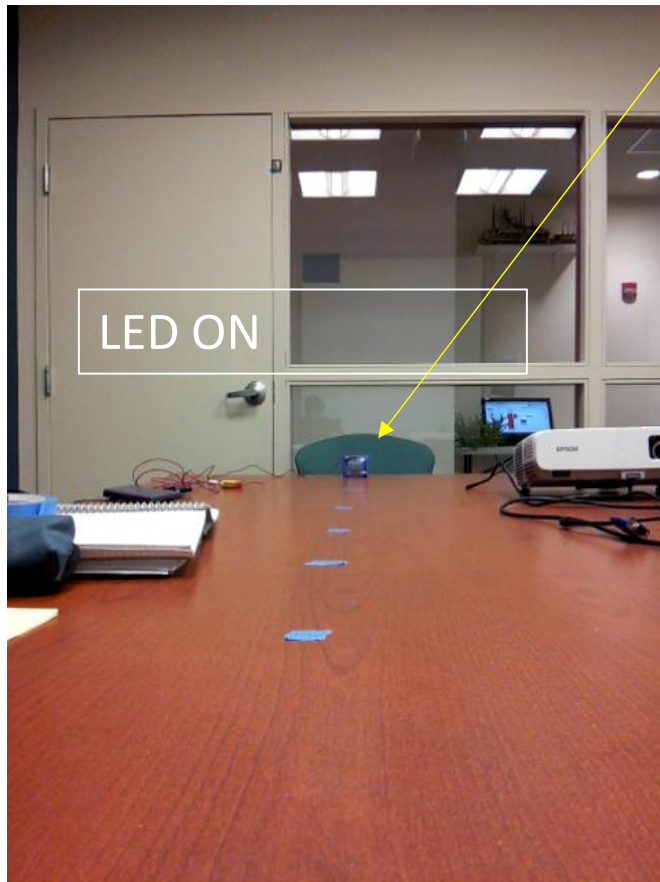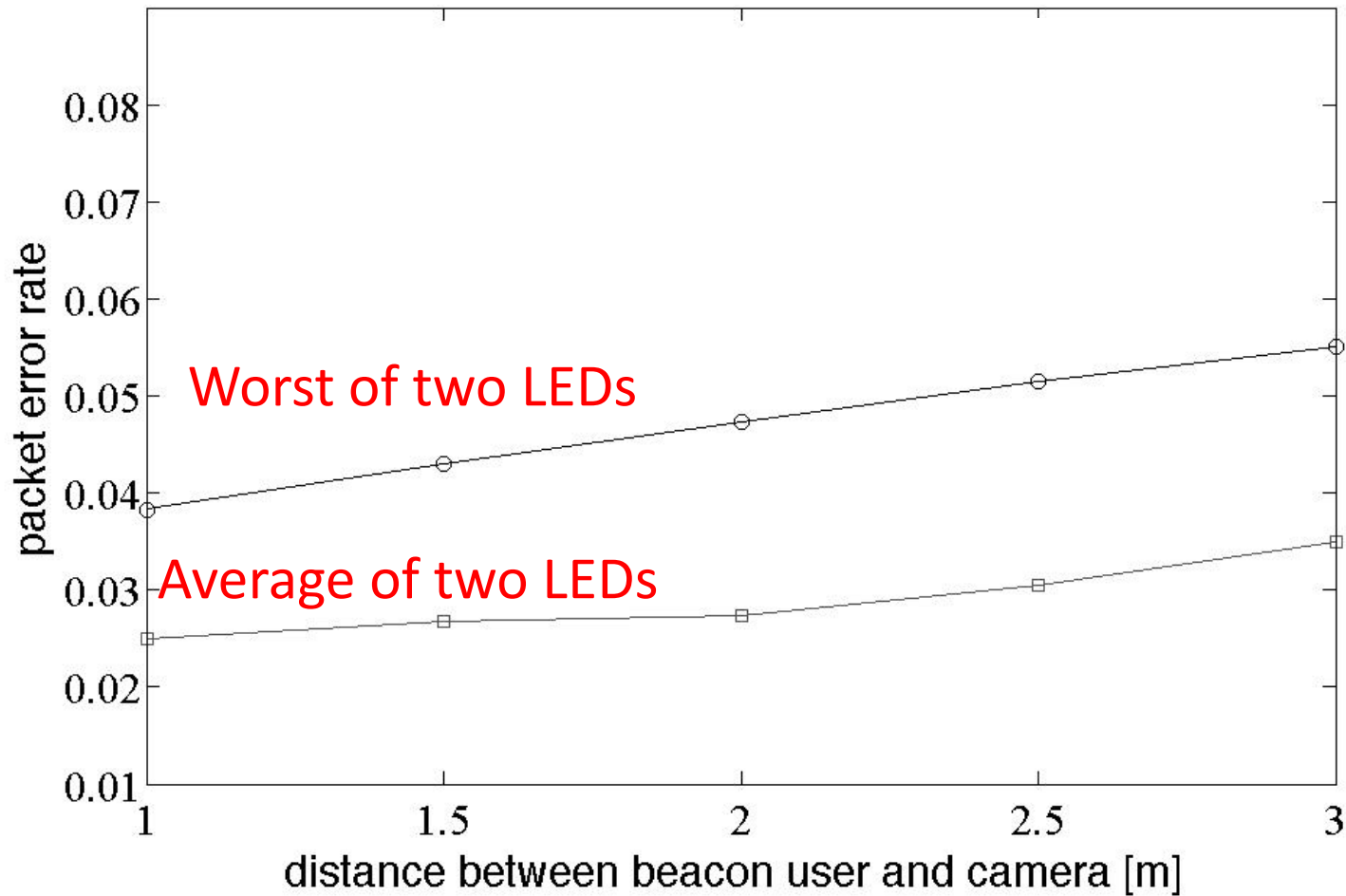
Available composing time

Accuracy

TPR v/s FPR at different
Correlation thresholds

(distance = 3m)

TPR = #true positives/(#true positives + #false negatives)
FPR = #false positives/(#false positives + # true negatives)

Experiment 2: Random bit stream

IR-LED transmitting a random bit-stream

LED ON

LED OFF

Packet error rate vs. distance

No error-control coding
Manually synchronized based on knowing start and stop time of transmission

Would people wear it?

Whose right is it?

Photographer vs. Privacy beacon user

Limitations and Future work

- Short range
- Does not work outdoor
- Energy optimization required for wearable devices

Future work:
- Add Bluetooth for intelligent device discovery
- Trigger optical element based on Bluetooth discovery
- Improve range through efficient transmission and processing

Summary

- Contributions
  - Identify an application area for light communication
  - Show the feasibility of communicating IR signals to camera
  - Conduct experiment towards understanding if *(a) a known IR signal can be reliably detected* and *(b)if the channel quality is sufficient for IR communication*
- Other applications
  - Send photo subject identities for more reliable tagging
  - Send an emergency signal to a camera surveillance system