Demo: LiShield: Privacy Protection of Physical Environment Against Photographing

Shilin Zhu*
University of California San Diego
shz338@eng.ucsd.edu

Chi Zhang*
University of Wisconsin-Madison
czhang296@wisc.edu

Xinyu Zhang
University of California San Diego
xiz368@eng.ucsd.edu

ABSTRACT

The ubiquity of mobile camera devices has been triggering an outcry of privacy concerns, whereas privacy protection still relies on the compliance of the photographer or camera hardware, which can hardly be guaranteed in practice. In this demo, we introduce LiShield, which automatically protects a physical scene against photographing, by illuminating it with smart LEDs flickering in a specialized waveform. We use a model-driven approach to optimize the waveform, so as to ensure protection against the (uncontrollable) cameras and potential image-processing based attacks. We have also designed mechanisms to unblock authorized cameras and enable graceful degradation under strong ambient light interference. This demo will show our prototype implementation, with simple on-site experiments that demonstrate how LiShield effectively destroys unauthorized photo capturing.

CCS CONCEPTS

• **Computer systems organization → Special purpose systems**; • **Security and privacy → Security services**; *Systems security*; • **Human-centered computing → Ubiquitous and mobile devices**; • **Computing methodologies → Computer vision**;

KEYWORDS

Privacy Protection; Visible Light; Camera; Computer Vision

1 INTRODUCTION

Cameras are now pervasive on consumer mobile devices, such as smartphones, tablets, drones, smart glasses, first-person recorders, *etc.* The ubiquity of these cameras, paired with pervasive wireless access, is creating a new wave of visual sensing applications, *e.g.*, autonomous photographer, quantified-self (life-logging), photo-sharing social networks, physical-analytics in retail stores, and augmented reality applications that navigate users across unknown environment. Zooming in the photo-sharing application alone, statistics report that 350 million photos/videos are uploaded to Facebook every day, majority of which are from mobile users [7]. Many of these applications automatically upload batches of images/videos online, with a simple one-time permission from the user. While these technologies bring significant convenience to individuals, they also trigger an outcry of privacy concerns.

Privacy is ultimately a subjective matter, and often varies with context. Yet many of the privacy-sensitive scenes occur in indoor environment, and are bound to specific locations. For example, recent user studies [2] showed that people's acceptability of being recorded by augmented reality glasses has a strong correlation with location. User studies of life-logging cameras [3] also indicate that 70.2% of the cases when the user disables capturing is associated with specific locations. In numerous real-world scenarios, cameras are forbidden, *e.g.*, concerts, theaters, museums, trade shows, hospitals, dressing rooms and exam rooms, manufacturing plants, *etc.* However, *visual privacy protection in such passive physical spaces still heavily relies on rudimentary approaches* like warning signs and human monitors, and there is no way to automatically enforce the requirements. In personal visual sensing applications like life-logging, even if a user were to disable the camera in private space (*e.g.*, bedroom and washroom), malware could perform remote reconnaissance and targeted visual theft by hijacking the victim's camera [8].

In this demo, we introduce LiShield, a system that thwarts photographing of sensitive indoor physical space, and automatically enforces location-bound visual privacy protection. LiShield safeguards the physical scenes against undesired recording without requiring user intervention, and without disrupting the human visual perception. Our key idea is to illuminate the environment using smart LEDs, which are intensity-modulated following specialized waveforms. We design the waveform in such a way that its modulation pattern is imperceptible by human eyes, but can disrupt the image sensors on mobile camera devices.

More specifically, our basic waveform follows an ON-OFF modulation, which causes the reflection intensity of the scene to "flicker" at high frequency. Digital cameras commonly adopt rolling-shutter image sensors, which sample the scene row by row during capturing. Consequently, LiShield will impose a striping effect on the captured image, as long as its flickering frequency exceeds the camera frame rate. To protect against a wide range of camera settings, we build a numerical model to explore the relation between the image quality degradation and the (uncontrollable) camera configurations (*e.g.*, exposure time). Accordingly, we derive common guidelines to maximize the effectiveness through waveform parameter configurations (*e.g.*, frequency, peak intensity, duty cycle). To further enhance the protection, we take two measures: *(i.)* scramble the color patterns, taking advantage of the array of multi-channel RGB chips commonly available on commercial smart LEDs; *(ii.)* randomize the waveform frequency to thwart exposure time manipulation that may circumvent the striping effect, while ensuring

*Co-primary authors.

MobiCom '17, October 16-20, 2017, Snowbird, UT, USA

ACM ISBN 978-1-4503-4916-1/17/10.
https://doi.org/10.1145/3117811.3119867

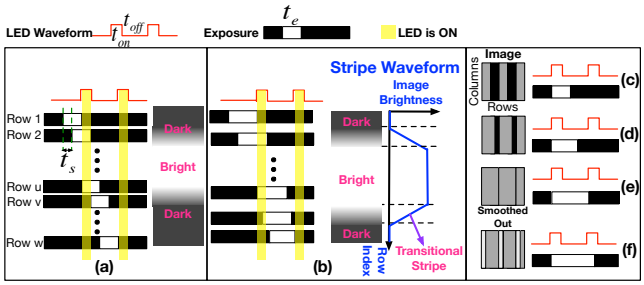

Figure 1: (a)-(b) Bright, dark and transitional stripes and their width changing with exposure time; (c)-(f) Stripe pattern of image changes under different exposure times.

no low-frequency components are generated that affect human perception.

In addition, LiShield can tailor the waveform for two special use cases: *(i.)* allowing an authorized camera, which shares secret configuration information with the LED, to recover the image or video frames it captures. *(ii.)* when strong ambient light interferes with the smart LED, LiShield cannot ensure full protection, but it can still emit structured light which embeds invisible "barcode" into the physical environment. The embedded information can convey a "no distribution" message, allowing online servers (*e.g.*, from Facebook and Instagram) to block and prevent the image from being distributed.

We have implemented LiShield based on a customized smart LED, which allows reconfiguration of intensity modulation waveforms on each color channel. Our experiments on real world scenes demonstrate that LiShield can corrupt the camera capturing to an illegible level, in terms of the image brightness, structure, and color. The impact is resilient against possible post-processing attacks, such as multi-frame combining and denoising. On the other hand, it enables authorized cameras to recover the image perfectly, as if no modulation is present. Even under strong sunlight/flashlight interferences, LiShield can still sneak barcode into the physical scenes which can be decoded with around 95% accuracy.

2 WORKING PRINCIPLE OF LISHIELD

Unlike professional or industrial cameras which may have global shutters that mimic human eyes to some degree, nearly all consumer digital cameras, pinhole cameras, and smartphones use the rolling shutter sampling mechanism [5], which is the main contributor to their high-frequency sensitivity. When capturing an image frame, a *rolling shutter camera exposes each row sequentially*. This effect has been leveraged to capture high-frequency optical signals for other purposes such as localization [4, 6, 9] and communication.

LiShield harnesses the disparity between cameras and eyes to disrupt the camera imaging without affecting human vision. It modulates a smart LED to generate high-frequency flickering patterns. The reflection intensity (or brightness) of target scene also flickers following the same pattern as the LED's illumination, albeit at reduced intensity due to reflection loss. LiShield uses the On-Off Keying (OOK) as the basic modulation waveform (Fig. 1), which does not require complicated analog front-ends and is widely supported by smart LEDs. Due to rolling-shutter sampling, the rows of pixels that are fully exposed in the ON period will be bright, and rows in the OFF period become dark, thus causing striped patterns on the captured image (Fig. 1(a)(b)). Partially exposed rows experience moderate brightness. Meanwhile, human eyes can only perceive the smooth averaged intensity, as long as the OOK frequency goes beyond 80 Hz [1]. LiShield aims to minimize the image capturing quality by optimizing the LED waveform, characterized by modulation frequency, intensity, and duty cycle.

In addition, commercial LED fixtures often comprise multiple LED bulbs/chips, and sometimes separate RGB channels to allow color adjustments. LiShield can turn different numbers of LED bulb/chip on to generate different intensities, and control the RGB channels of the LEDs to vary the color. Therefore, LiShield's flickering waveform is staircase-shaped on-off patterns, running independently in 3 color channels.

LiShield should still maintain its protection while allowing authorized users to capture the same scene simultaneously without distortion. LiShield's solution leverages a secure side channel (*e.g.*, visible light communication [10, 11]) between authorized users and the smart LED, which conveys secret information such as frame timing and waveform parameters. To authorize a camera to capture a dynamic scene (Fig. 2), each individual frame within the video must be recoverable. To achieve this, the authorized camera needs to convey its exposure time setting to the smart LED via the secure side channel, and synchronize its clock (for controlling capturing time) with the smart LED's clock (for controlling the waveform). State-of-the-art time synchronization mechanisms through visible light or wireless side-channels can already achieve μs of accuracy, sufficient to synchronize the LiShield smart LED with the camera at a resolution finer than the rolling shutter period (typically tens of μs). The corresponding flickering frequency can be varied on a frame by frame basis, making it impossible for an attacker to resolve the correct exposure time by trial-and-error. When the target scene is static, it requires the authorized user to capture a few complementary frames to recover the scene as depicted in Fig. 3. Meanwhile, frequency and intensity randomization can still be employed in each frame to ensure robustness. While it does require recording a very short video, the process is extremely short (200ms at most) and barely noticeable.

In case strong ambient interference may degrade LiShield's protection, LiShield embeds barcodes in images/videos captured by the attacker to convey privacy policies and ensures they are detectable even after common post-processing.

3 DEMO SETUP AND REQUIREMENT

In the demo, we will show our LiShield hardware prototype, and encourage the audience to take photos using their smartphones while experiencing the corruption effects under LiShield. We will also demonstrate how an authorized camera (which we bring by ourselves) can circumvent the corruption effects. Besides the AC power and a table, no other facility is needed. The setup time is around 10 minutes.

Fig. 5 shows our LiShield prototype, and the target scenes containing 5 capture-sensitive objects (document and painting are 2-D objects and others are all 3-D objects). We mount the LED inside a diffusive plastic cover similar to conventional ceiling light covers. We use a programmable motor to hold the camera and control

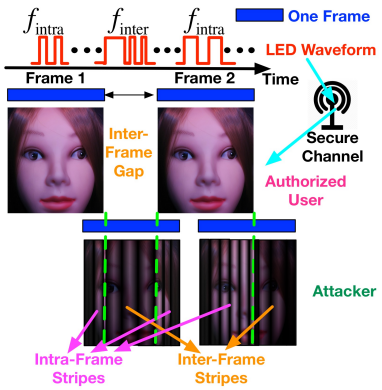

Figure 2: Enabling authorized users to capture dynamic scenes while corrupting unauthorized users.

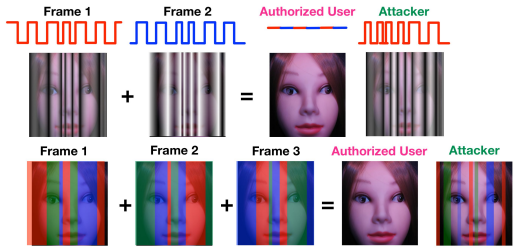

Figure 3: The impact of multi-frame recovery on authorized user and attacker, respectively.

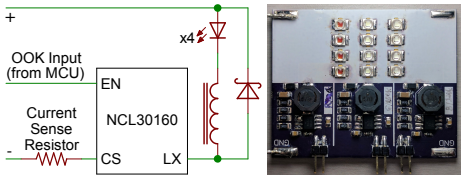

Figure 4: Simplified circuit diagram and photo for the smart LED module.

its distance/orientation, in order to create static or dynamic scene setup in a repeatable manner.

We build our smart bulb based on the same topology as those COTS LED bulbs. For safety, we use 19V DC laptop power supplies instead of wall AC power, and NCL30160 LED drivers which allow dimming at nearly 100 kHz with arbitrary OOK waveform. The smart bulb has built-in independent RGB/white channels for controlling color/intensity. Each channel can be controlled by a separate waveform, with 4 LED chips in series, at driving current of 800 mA. In total, the 3 channels consume approximately 25 W peak power, close to common office LED troffer fixtures. However, since LiShield's OOK waveform has a duty cycle much lower than 1, the actual perceptible brightness is significantly lower. As a result, multiple LED modules can be used to improve light intensity. Fig. 4 depicts the circuit for each color channel and shows a photo of the whole module. The dimming input signals of each channel are controlled by an STM32 micro-controller unit (MCU), which generates the OOK waveform as specified by LiShield. For flexible reconfiguration, we generate digitized waveforms in MATLAB on

Figure 5: Experimental setup and multiple scenes we used.

a laptop or Android app on a smartphone instead, which are then passed to the MCU via USB.

4 CONCLUSION

Privacy protection in passive indoor environment has been an important but unsolved problem. In this demo we present LiShield, which uses smart-LEDs and specialized intensity waveforms to disrupt unauthorized cameras, while allowing authorized users to record high-quality image and video. We implemented and evaluated LiShield under various representative indoor scenarios, which demonstrates LiShield's effectiveness and robustness. We consider LiShield as the first exploration of automatic visual privacy enforcement and expect it can inspire more research along the same direction.

REFERENCES

[1] Stephen J. Anderson and David C. Burr. 1985. Spatial and temporal selectivity of the human motion detection system. *Vision Research* 25, 8 (1985), 1147 – 1154.

[2] Tamara Denning, Zakariya Dehlawi, and Tadayoshi Kohno. 2014. In Situ with Bystanders of Augmented Reality Glasses: Perspectives on Recording and Privacy-mediating Technologies. In *Proc. of ACM CHI*.

[3] Roberto Hoyle, Robert Templeman, Steven Armes, Denise Anthony, David Crandall, and Apu Kapadia. 2014. Privacy Behaviors of Lifeloggers Using Wearable Cameras. In *Proc. of ACM UbiComp*.

[4] Ye-Sheng Kuo, Pat Pannuto, Ko-Jen Hsiao, and Prabal Dutta. 2014. Luxapose: Indoor Positioning with Mobile Phones and Visible Light. In *Proc. of ACM MobiCom*.

[5] QImaging. 2014. Rolling Shutter vs. Global Shutter. (2014). https://www.qimaging.com/ccdorscmos/pdfs/RollingvsGlobalShutter.pdf

[6] Niranjini Rajagopal, Patrick Lazik, and Anthony Rowe. 2014. Visual Light Landmarks for Mobile Devices. In *Proc. of ACM/IEEE IPSN*.

[7] Social Pilot. 2016. 125 Amazing Social Media Statistics You Should Know. (2016). https://socialpilot.co/blog/125-amazing-social-media-statistics-know-2016/

[8] R. Templeman, Z. Rahman, D. Crandall, and A. Kapadia. 2013. PlaceRaider: Virtual Theft in Physical Spaces With Smartphones. In *Network and Distributed System Security Symposium (NDSS)*.

[9] Chi Zhang and Xinyu Zhang. 2016. LiTell: Robust Indoor Localization Using Unmodified Light Fixtures. In *Proc. of ACM MobiCom*.

[10] Jialiang Zhang, Chi Zhang, Xinyu Zhang, and Suman Banerjee. 2016. Towards a Visible Light Network Architecture for Continuous Communication and Localization. In *Proc. of ACM VLCS*.

[11] Jialiang Zhang, Xinyu Zhang, and Gang Wu. 2015. Dancing with Light: Predictive In-frame Rate Selection for Visible Light Networks. In *Proc. of IEEE INFOCOM*.