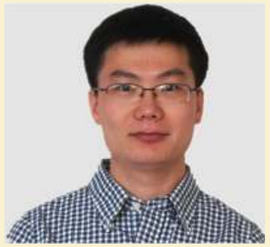
UC San Diego
JACOBS SCHOOL OF ENGINEERING
Computer Science and Engineering

THE UNIVERSITY of WISCONSIN MADISON

LISHIELD: AUTOMATING VISUAL PRIVACY PROTECTION USING A SMART LED


Shilin Zhu


Chi Zhang


Xinyu Zhang

Presented by Kai Zhang

VISUAL PRIVACY PROTECTION IS URGENT

We don't want to be photographed!

PASSIVE PHYSICAL OBJECTS

STYLE

le

A MALE SECURITY GUARD USES STORE surveillance cameras to zoom in on the cleavage of an unsuspecting

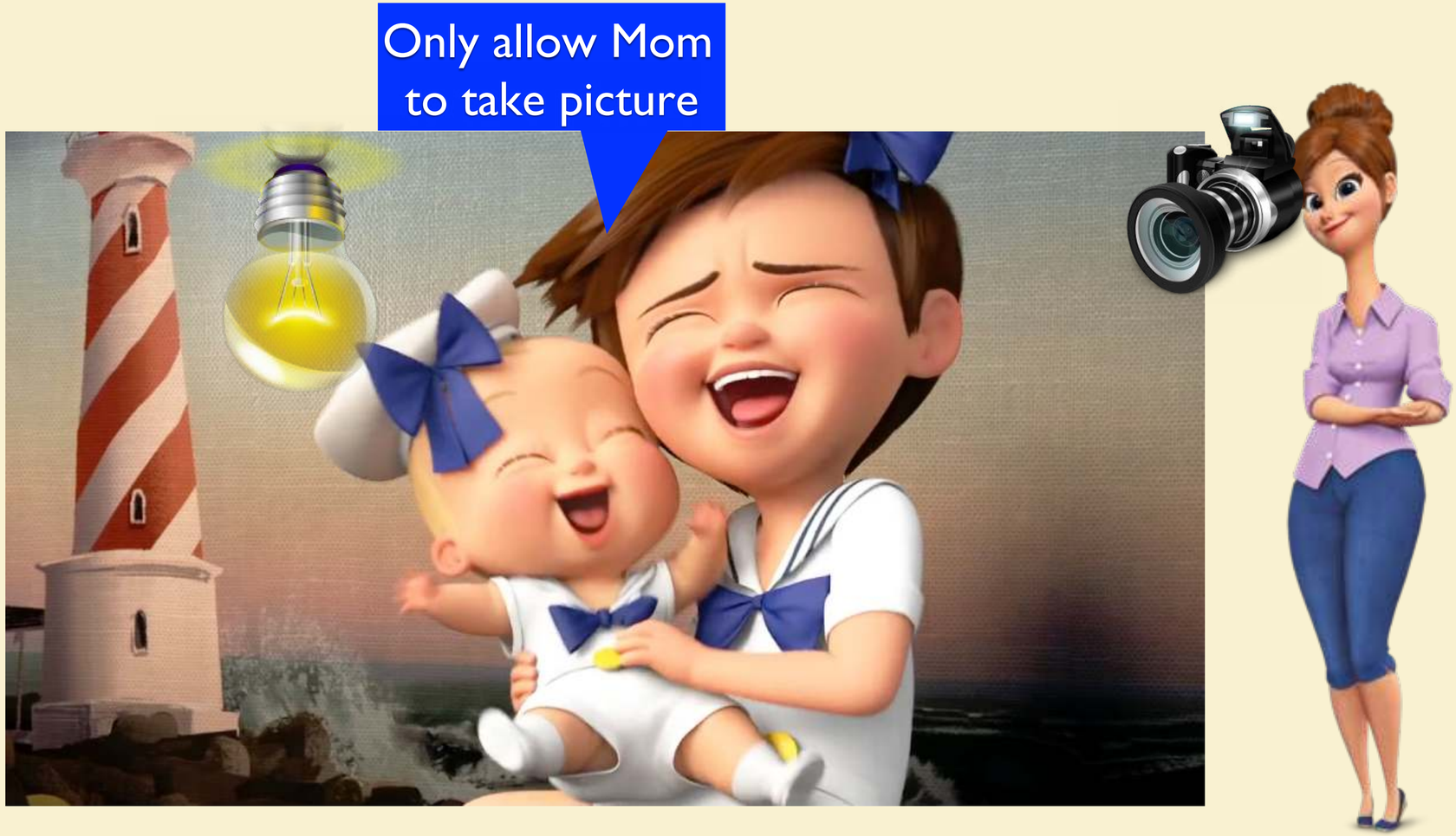
jockstrap, is one plaintiff in a pending lawsuit against the company for invasion of privacy. "I worked real hard for them and

EXISTING RUDIMENTARY APPROACHES

LISHIELD SYSTEM OVERVIEW

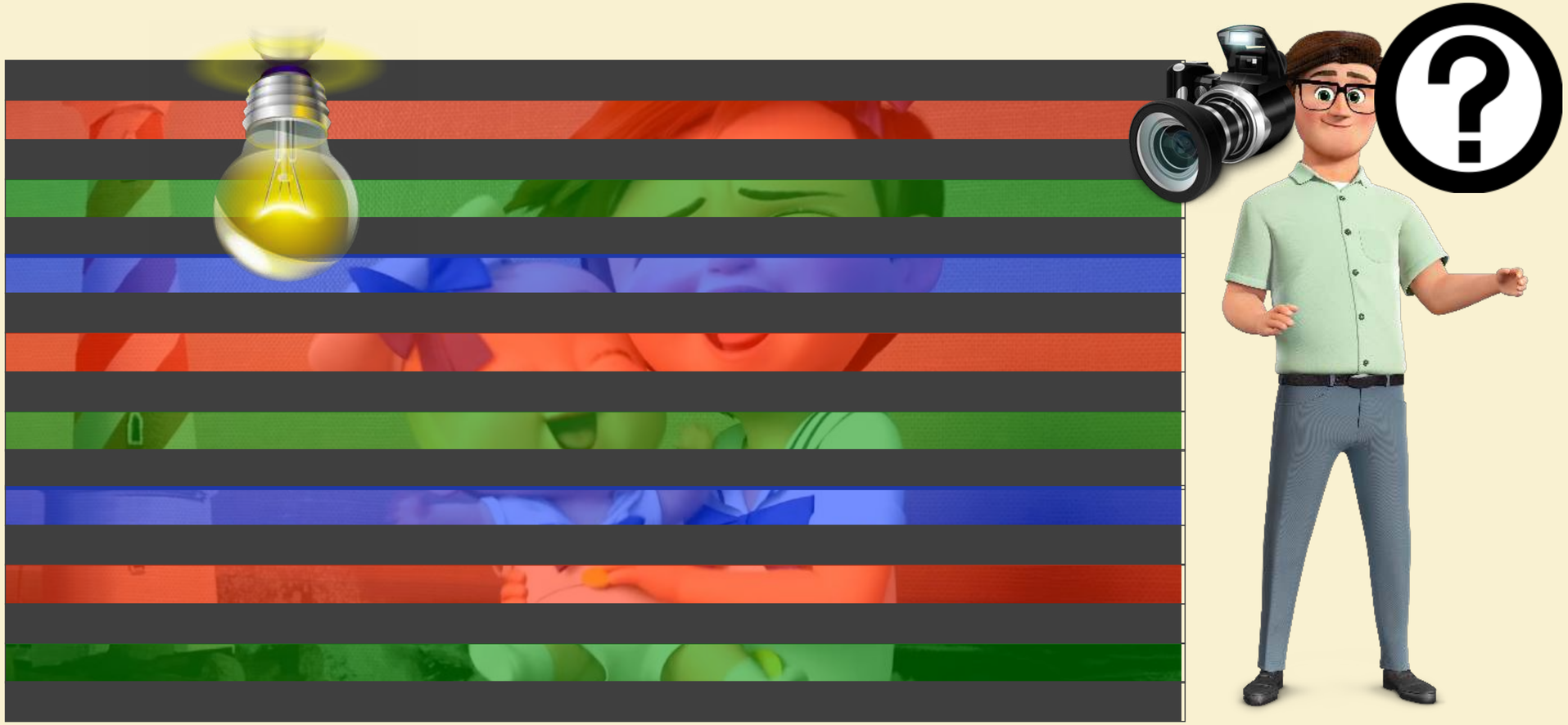
- Corruption: block illegal camera users
- Authorization: unblock legal camera users
- Watermarking: conveying ‘no distribution’ message

AUTHORIZATION



PICTURE TAKEN BY MOM

AUTHORIZATION



PICTURE TAKEN BY OTHER PEOPLE

Upload fail.
Image is
confidential

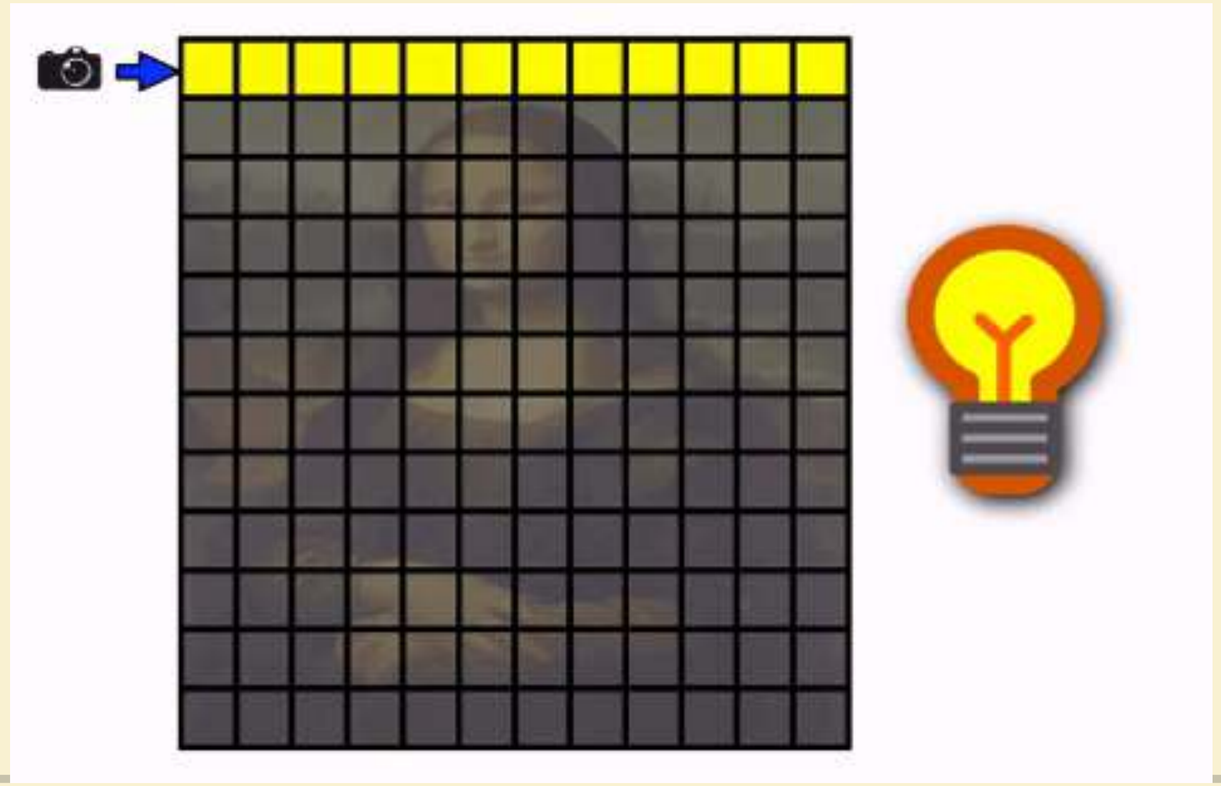
CAMERA: ROLLING SHUTTER

Intensity

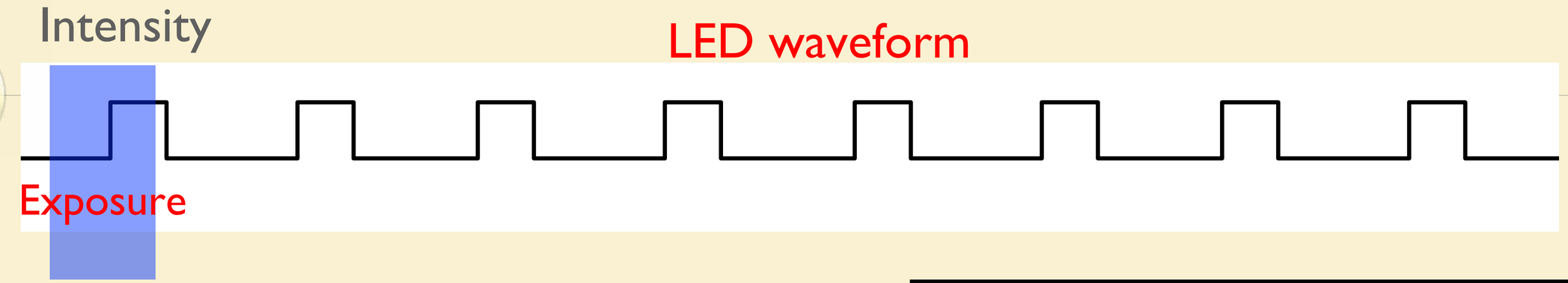
Normal indoor lights

Exposure

Time

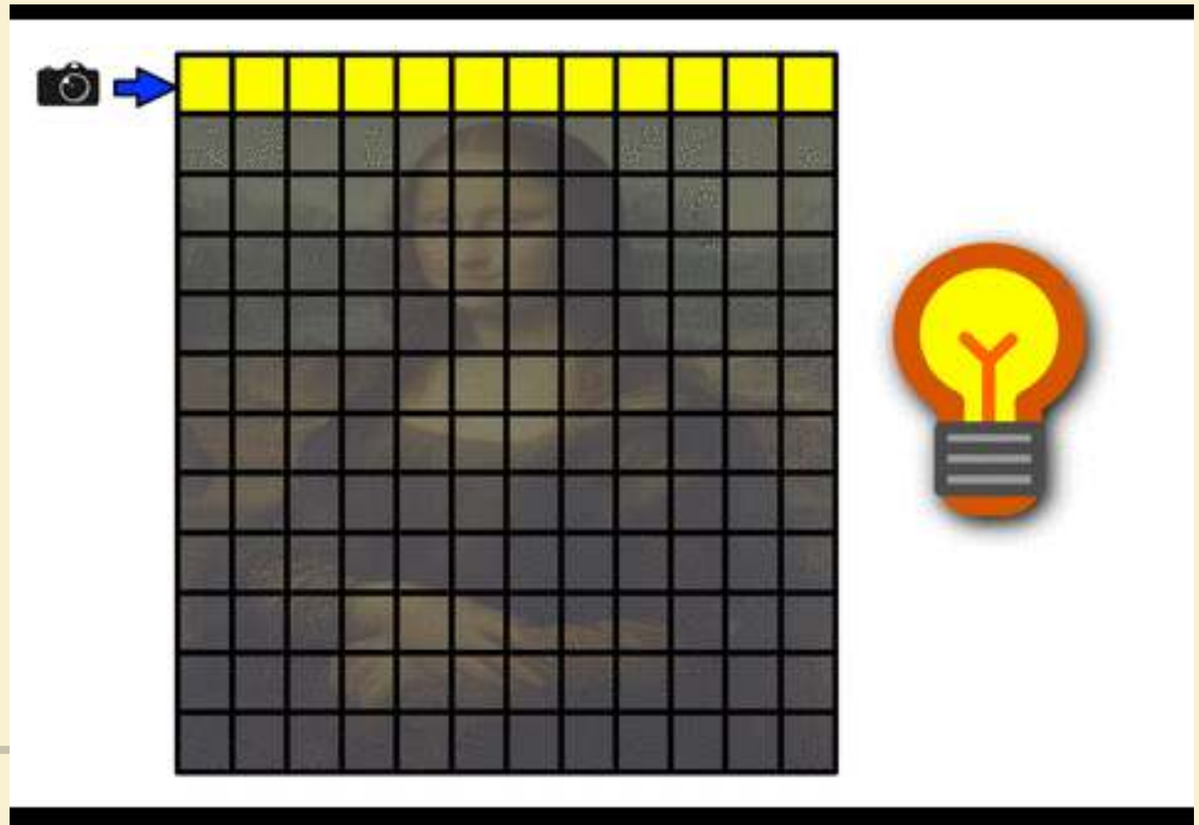


ROLLING SHUTTER + LIGHT WAVEFORM



Black-white waveform

RGB waveform



CHALLENGE #1: WAVEFORM IS TRANSPARENT TO HUMAN EYES

Intensity

Time

LED WAVEFORM

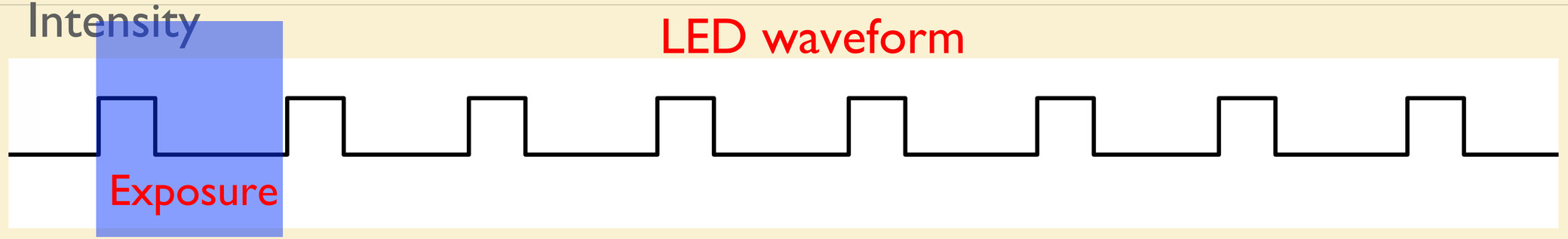
Intensity

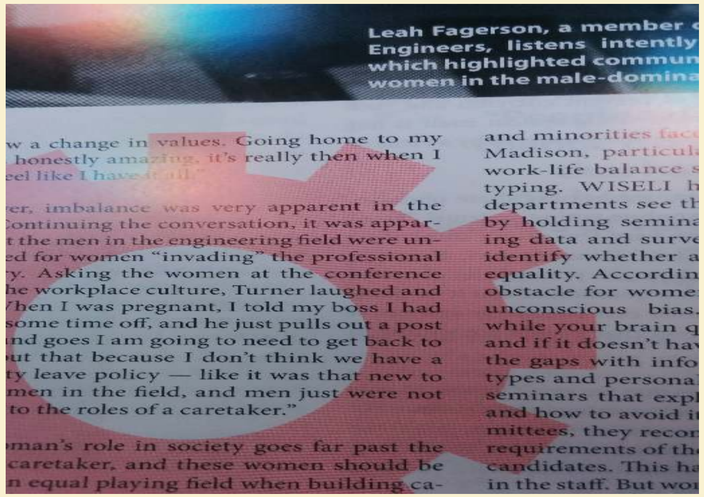
Time

f > 100Hz

PERCEIVED BY HUMAN EYES

CHALLENGE #2: ROBUSTNESS AGAINST CAMERA MANIPULATION





$$T(wave) = T(exp)$$

Stripe pattern under different exposure times

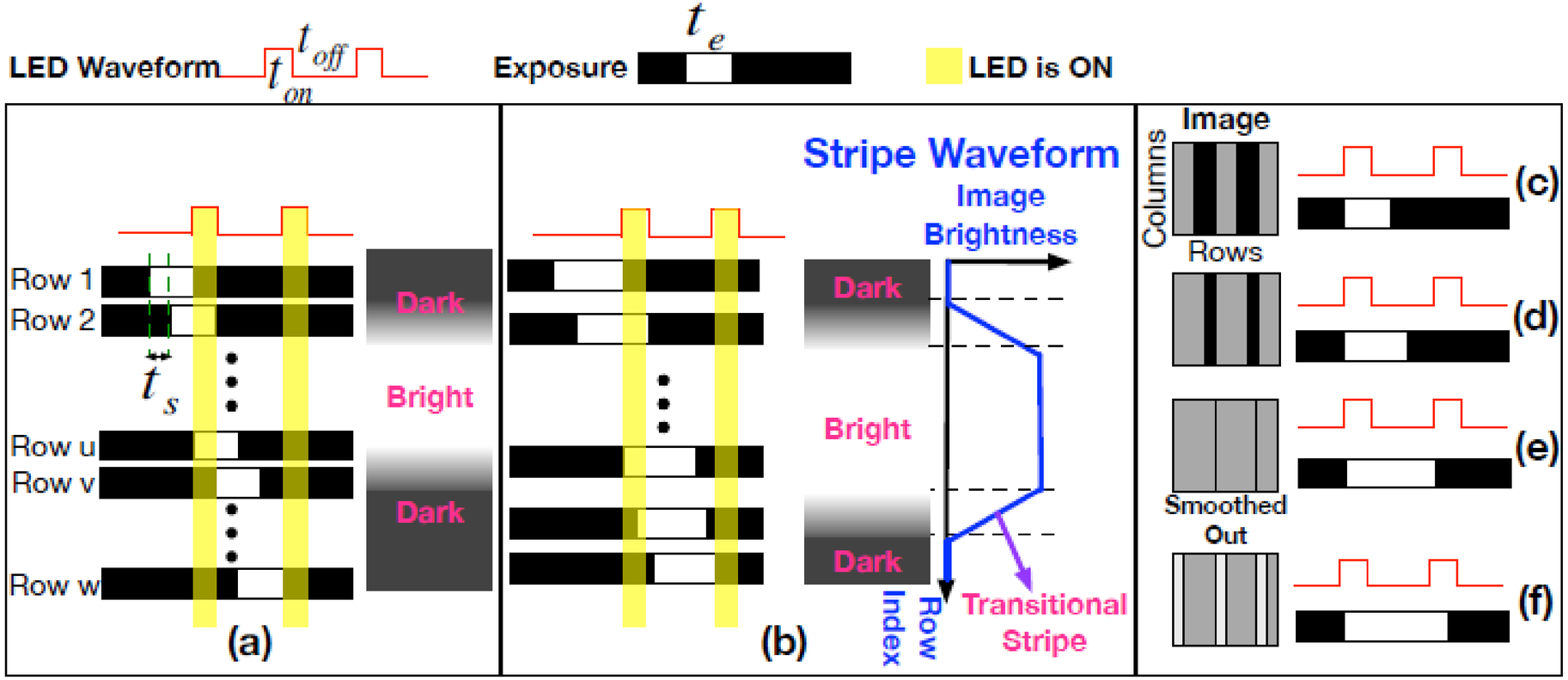


Figure 1: (a)-(b) Bright, dark and transitional stripes and their width changing with exposure time; (c)-(f) Stripe pattern of image changes under different exposure times.

Decomposing the image

For convenience, denote the period of the light source as $t_l = t_{\text{on}} + t_{\text{off}}$, and duty cycle as $D_c = t_{\text{on}}/t_l$. For pixel j in row i which starts exposure at time t_i, its light accumulation would be:

$$Q(i,j) = \alpha_{i,j} \int_{t_i}^{t_i+t_e} \pi_l(\tau) d\tau \tag{1}$$

where $\alpha_{i,j}$ is the aggregated path-loss for pixel (i,j), including attenuation and reflection on the photographed object, and $\pi_l(\tau)$ represents the illumination waveform of the LED:

$$\pi_l(\tau) = \begin{cases} I_p, & 0 < \tau \bmod t_l \leqslant t_{\text{on}} \\ 0, & t_{\text{on}} < \tau \bmod t_l \leqslant t_l \end{cases} \tag{2}$$

Decomposing the image

$$Q_B(i,j)=\begin{cases}\alpha_{i,j}I_p(Nt_{\text{on}}+t_{\text{rem}}), & 0<t_{\text{rem}}\leqslant t_{\text{on}}\\ \alpha_{i,j}I_p(N+1)t_{\text{on}}, & t_{\text{on}}<t_{\text{rem}}\leqslant t_l\end{cases} \tag{3}$$

$$W_B=|t_{\text{rem}}-t_{\text{on}}|/t_s \tag{4}$$

$$Q_D(i,j)=\begin{cases}\alpha_{i,j}I_pNt_{\text{on}}, & 0<t_{\text{rem}}\leqslant t_{\text{off}}\\ \alpha_{i,j}I_p(Nt_{\text{on}}+t_{\text{rem}}-t_{\text{off}}), & t_{\text{off}}<t_{\text{rem}}\leqslant t_l\end{cases} \tag{5}$$

$$W_D=|t_{\text{rem}}-t_{\text{off}}|/t_s \tag{6}$$

Optimizing the LED waveform

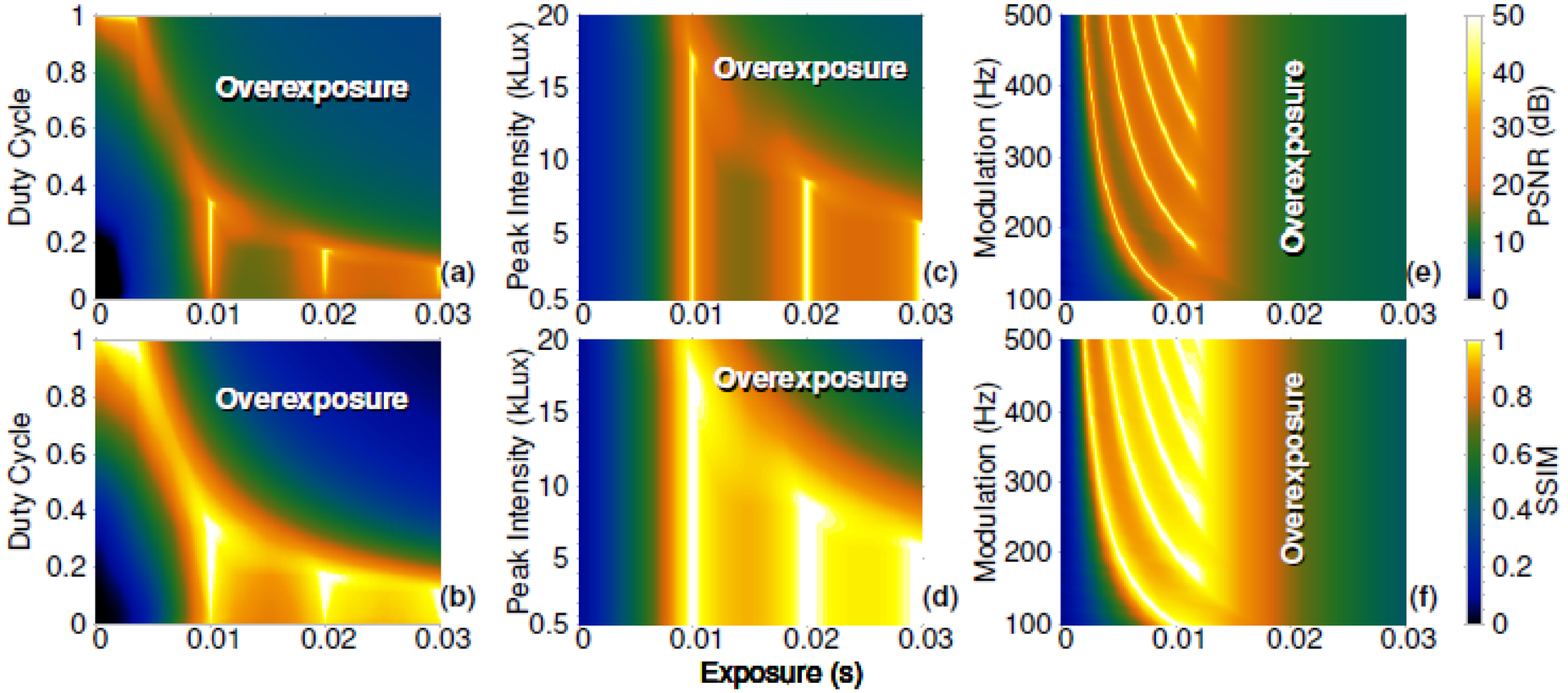


Figure 2: PSNR and SSIM with respect to exposure time, LED intensity, duty cycle, and modulation frequency.

Optimizing the LED waveform

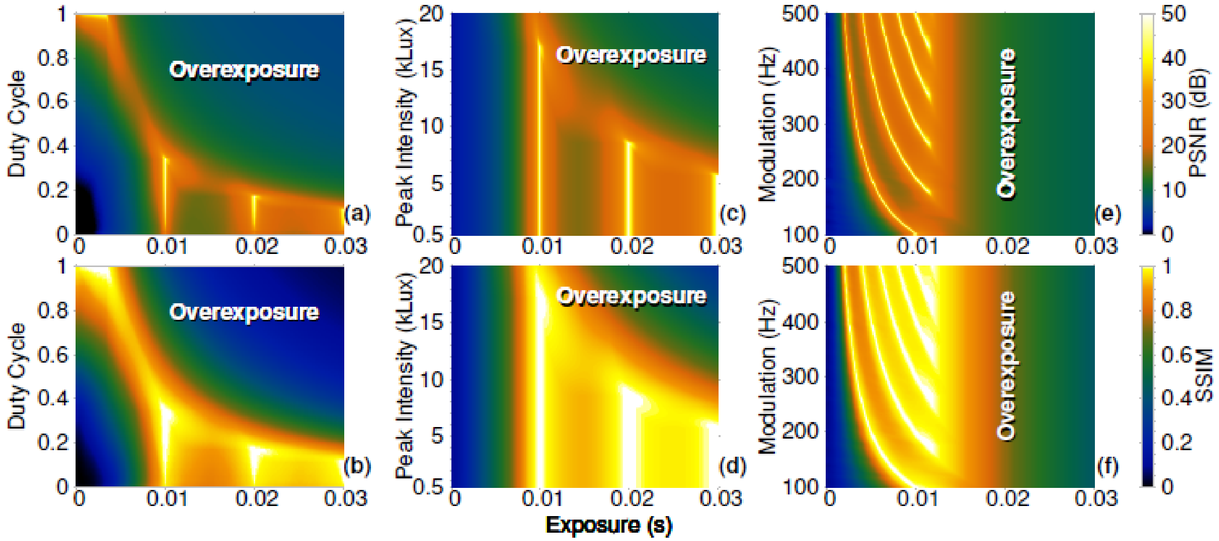


Figure 2: PSNR and SSIM with respect to exposure time, LED intensity, duty cycle, and modulation frequency.

1. A single frequency cannot ensure robust protection.
2. LiShield should prevent attackers from using long exposures.
3. LiShield should keep a high peak intensity to expand the overexposure zone.
4. Duty level should be kept at a modulate level.

Frequency scrambling

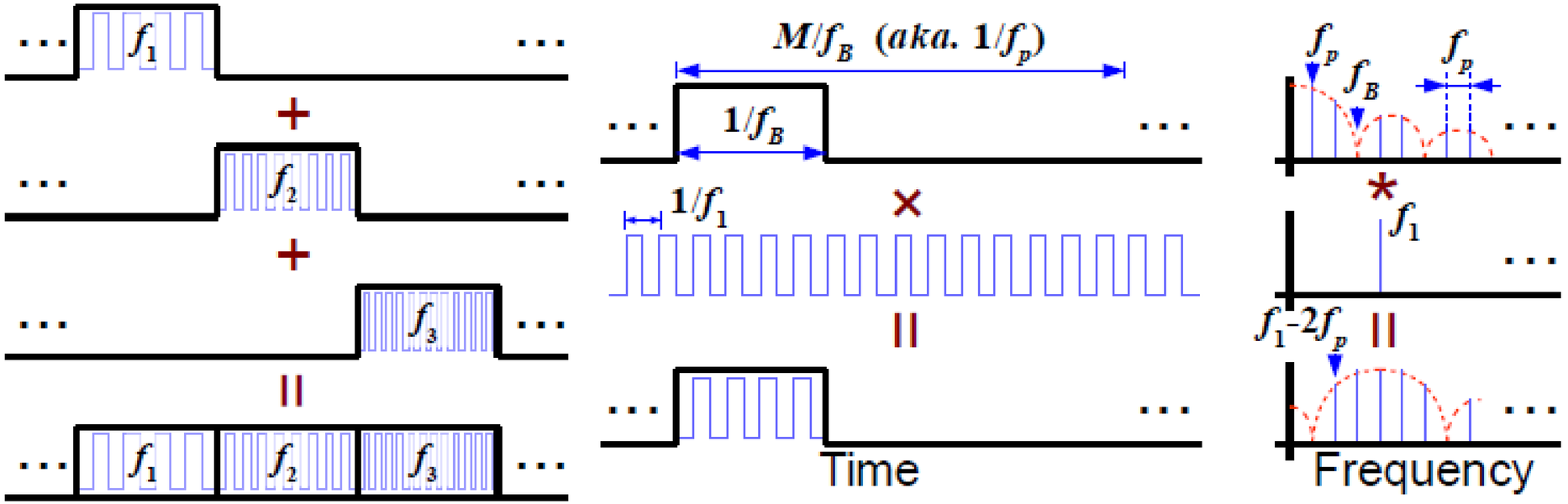


Figure 3: Decomposition of frequency randomization waveform and modulation generating side lobes.

$$f_n = f_B + (n-1)\Delta f, n \in 2, 3, \ldots, M,$$

CHALLENGE #2: ROBUSTNESS AGAINST CAMERA MANIPULATION

Intensity

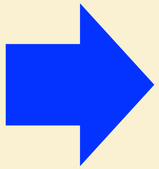
LED waveform

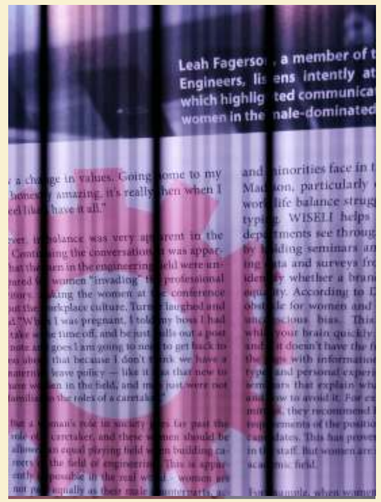
Exposure

Time

$$T(wave) \neq T(exp)$$

CHALLENGE #3: ROBUSTNESS AGAINST MULTI-FRAME RECOVERY





LED WAVEFORM

Illumination Intensity Randomization

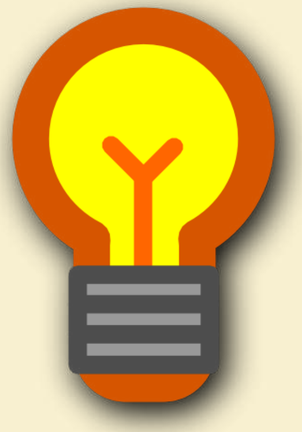
uncorrelated after the randomization. Then the probability that one row gets any illumination is $p = t_{\text{on}}/(t_{\text{on}} + t_{\text{off}}) = D_c$. Observe that on average same intensities would reappear approximately every K frames, the possibility of combining L frames to fully recover an image of the static scene is thus:

$$P_{\text{rec}} = \begin{cases} \left[1 - (1 - D_c)^{L/K}\right]^{m} & \text{(monochrome)} \\ \left[1 - (1 - D_c)^{L/K}\right]^{3m} & \text{(RGB)} \end{cases} \tag{8}$$

Therefore, achieving a given level of P_{rec} becomes increasingly difficult as D_c and K increases, and for higher camera resolution (larger m). For example, to have $P_{\text{rec}} = 90\%$ for $D_c = 0.5$ and $m = 2448$ for 8-mega-pixel cameras, the attacker needs $L = 300$ frames under $K = 10$, and ~ 3000 frames under $K = 100$. For lower duty cycles,

CAMERA AUTHORIZATION

CAMERA CAN RECOVER IMAGES GIVEN THE LED WAVEFORM



LiShield

I'm authorized

Verified

I'm generating this waveform

Gotcha

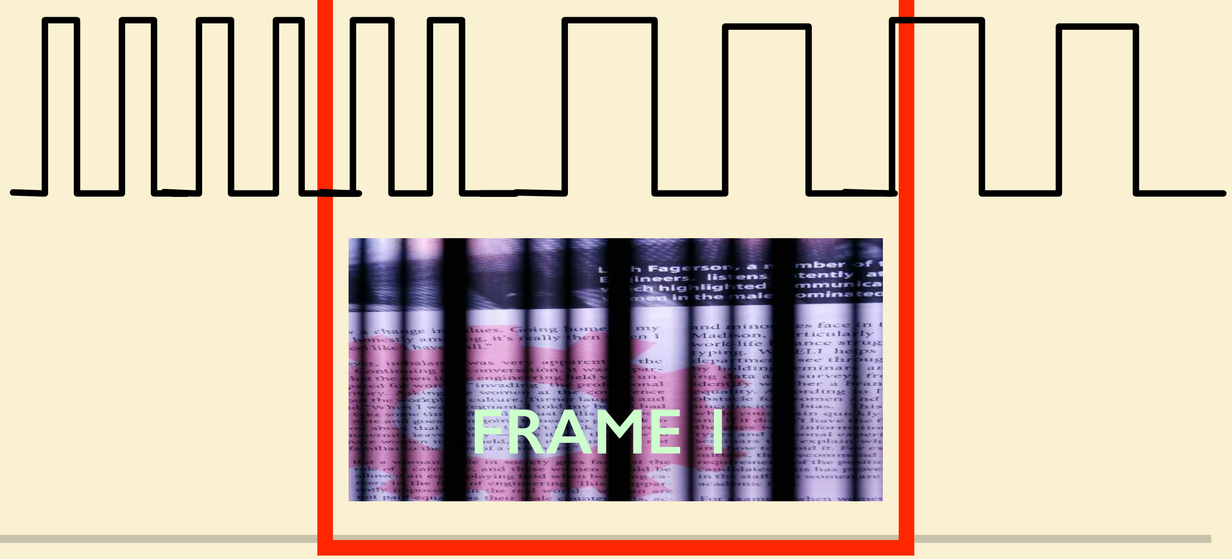
Authorized CAM

Challenge: How to unblock one person while keep blocking the others?

Authorized User

Attacker

LED WAVEFORM



Sometimes sunlight coming inside from windows,
LED can have little influence on image quality.

What should we do?

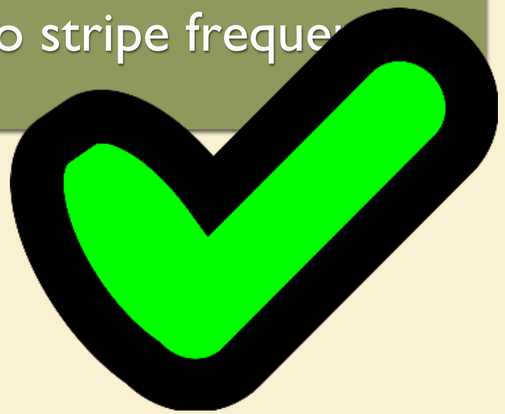
WATERMARKING

WATERMARK ENCODER

Affected by scene and ambient light noise

Vary with camera exposure

Ratio of two stripe freque



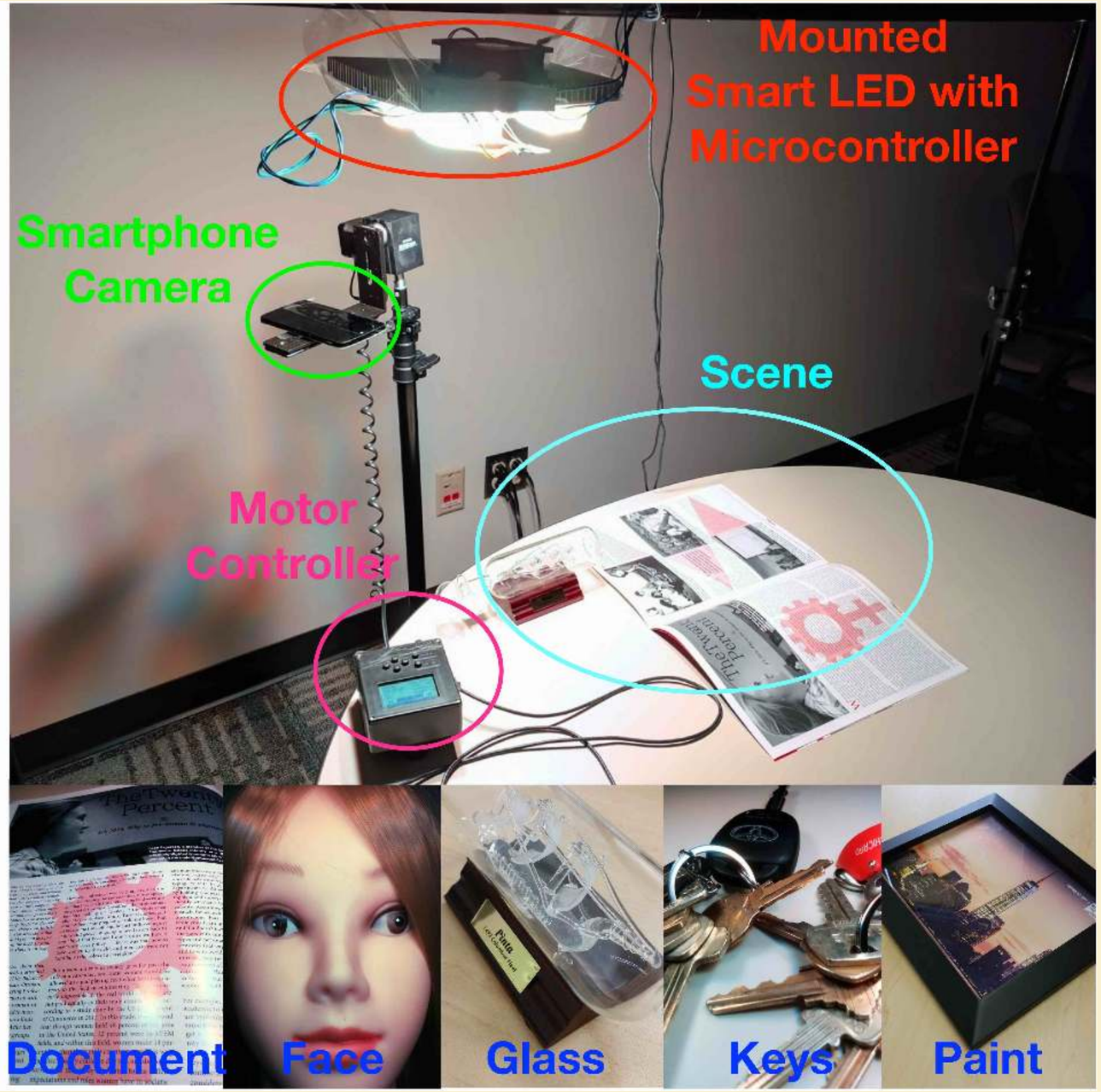
Vary with camera sampling rate

IMPLEMENTATION

- LED can generate OOK waveform specified by LiShield's image corruption and watermarking modules
- Authorization is implemented on Android

EXPERIMENTAL SETUP

- Various privacy-sensitive objects
- Metrics: PSNR, CW-SSIM, CIEDE2000

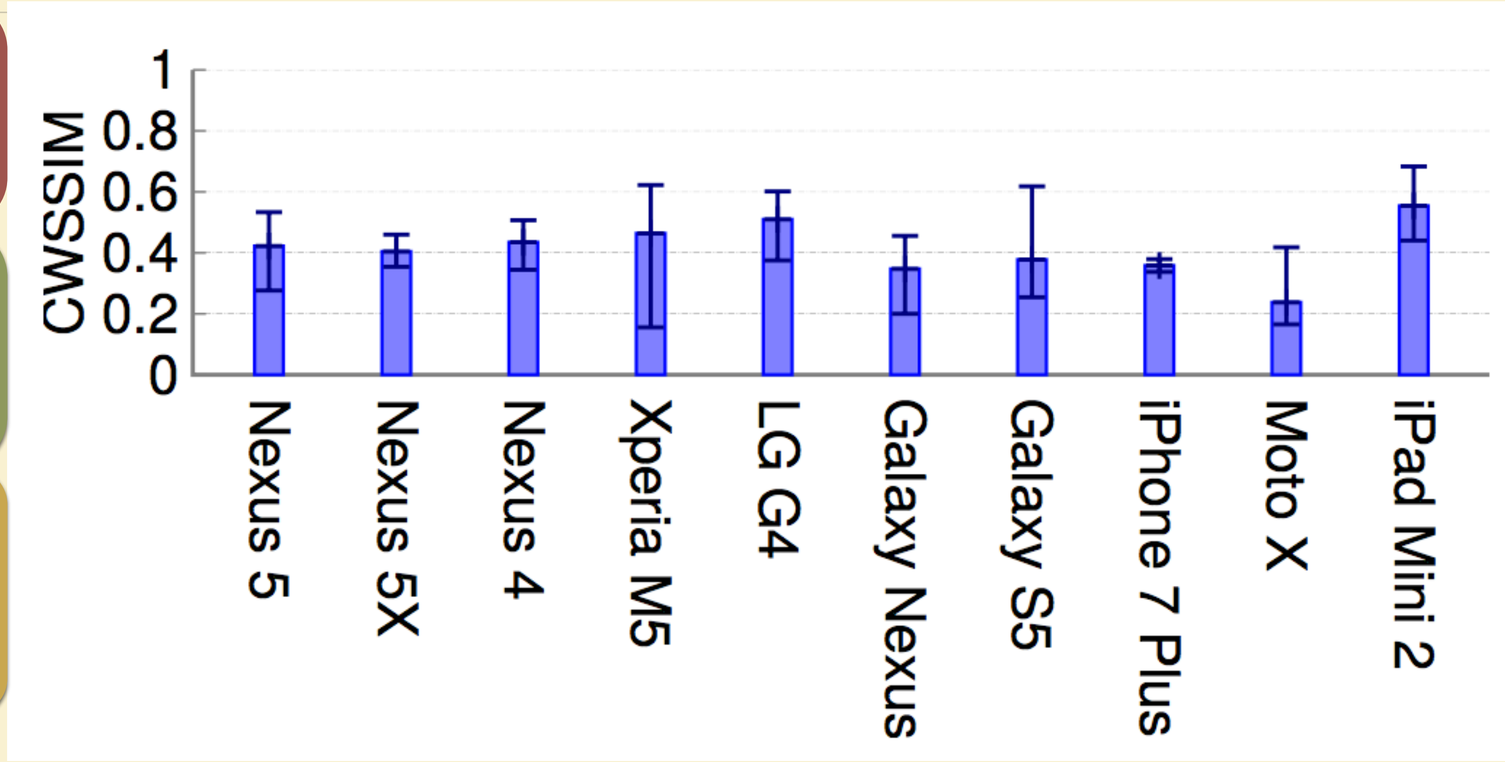


RESULT #1: QUALITY DEGRADATION

PSNR = 6 dB (>25 dB required)

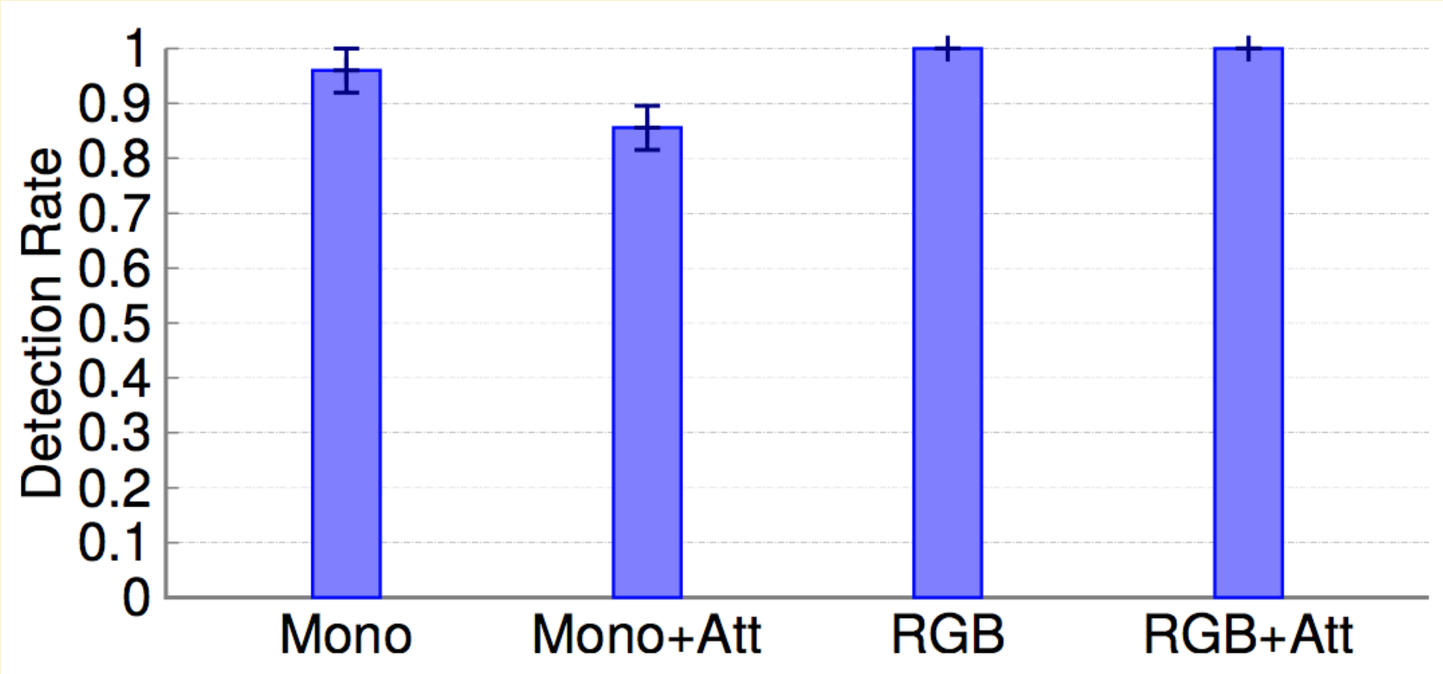
CW-SSIM = 0.3 (>0.9 required)

CIEDE2000 = 35 (<4 required)



RESULT #2: CAMERA AUTHORIZATION

RESULT #3: WATERMARKING



False alarm rate < 5%
Average detection rate > 90%

RESULT #4: ROBUSTNESS AGAINST ATTACKS AND ENVIRONMENTS

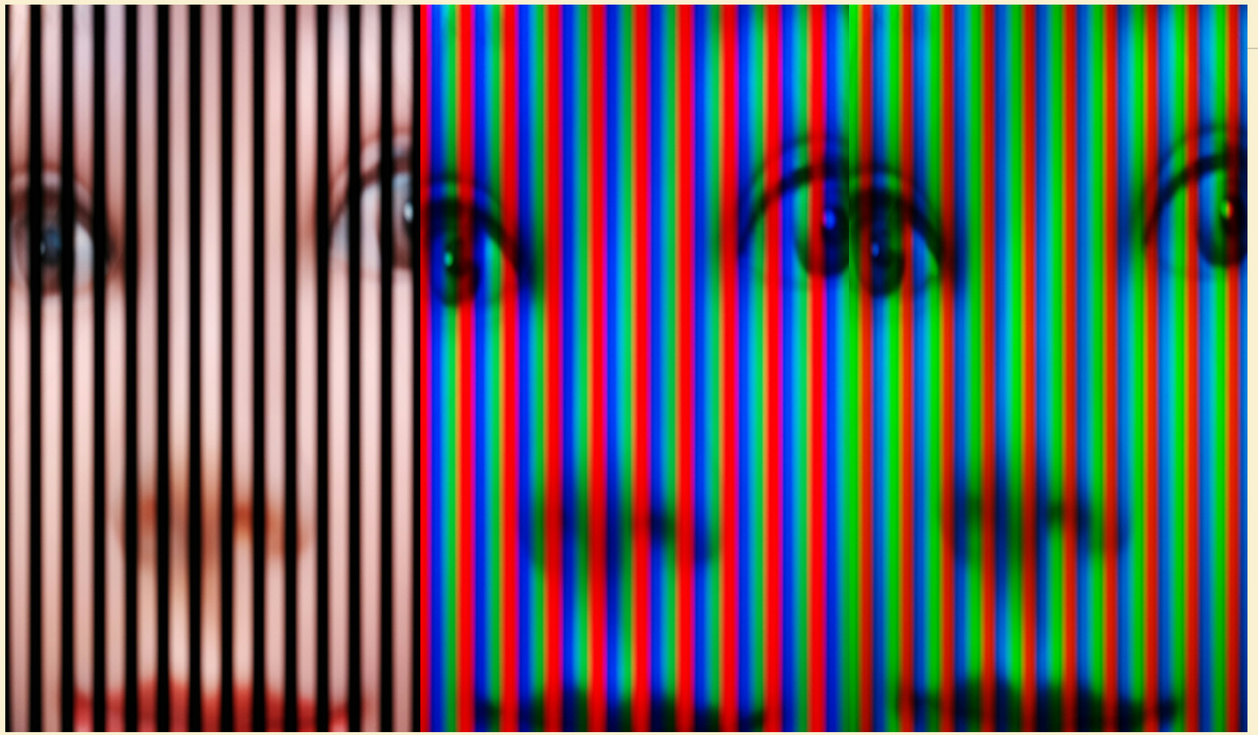
LiShield is robust against camera manipulation and multi-frame recovery

LiShield is robust against post-capture repairing algorithms

LiShield is robust against normal ambient lights

LiShield is robust against long distance using multiple LEDs

RESULT #5: SIDE BENEFITS



Color stripes destroy automatic white balance

Dynamic scene reduces space of exposure manipulation

CONCLUSION

- LiShield is a cost-effective, automatic, and easy-to-setup system enabling privacy protection against illegal cameras
- We design an authorization scheme to unblock specific user
- Watermarking adds ‘no distribution’ message recognizable by online servers

Fast setup

Low cost

Effective protection

我的看法

优点：
如何提高系统的干扰程度：细致的理论推导与仿真
实验

限制：
对Global shutter camera无效