ScreenID: Enhancing QRCode Security by Fingerprinting Screens

Yijie Li#, Yi-Chao Chen#, Xiaoyu Ji*, Hao Pan#, Lanqing Yang#,

Guangtao Xue#, Jiadi Yu#

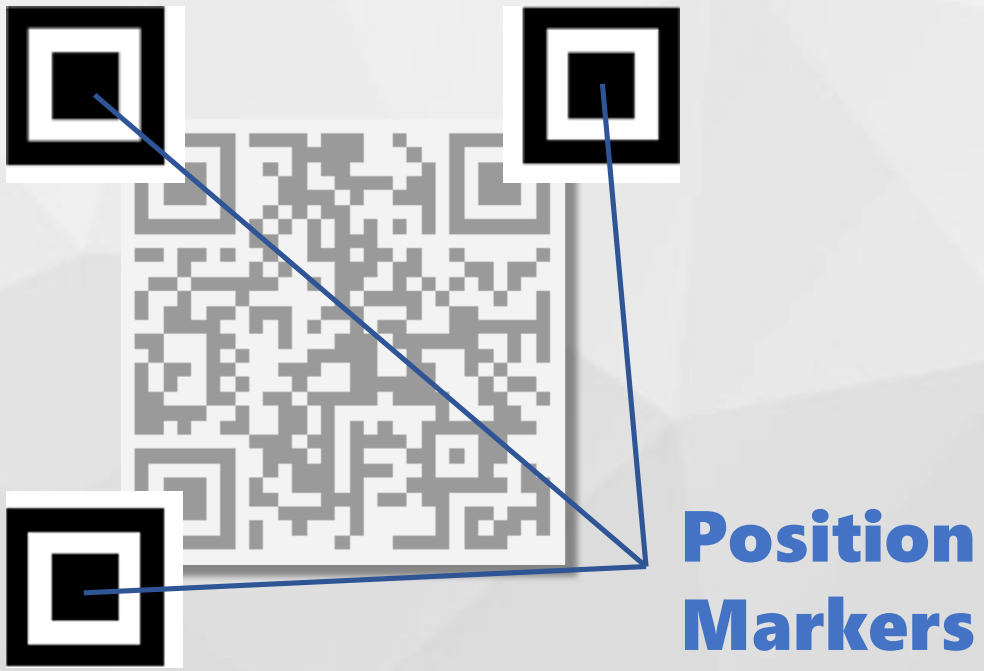
Shanghai Jiao Tong University#

Zhejiang University*

QR Code

Q R Code

Quick Response Code


Position
Markers

11M households scan a QR code in USA in 2020

In China, 50% users scan QR codes per week.

SouthEast Asia and India are the largest region to scan QR codes.

Australia has a 90% mobile penetration.

QR Code is becoming popular!

QR Code is becoming popular!

Payment

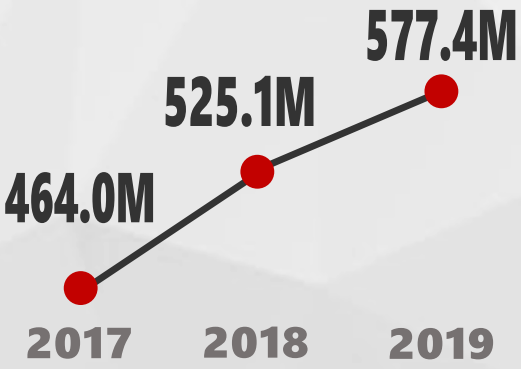
Advertisements

Social E-cards

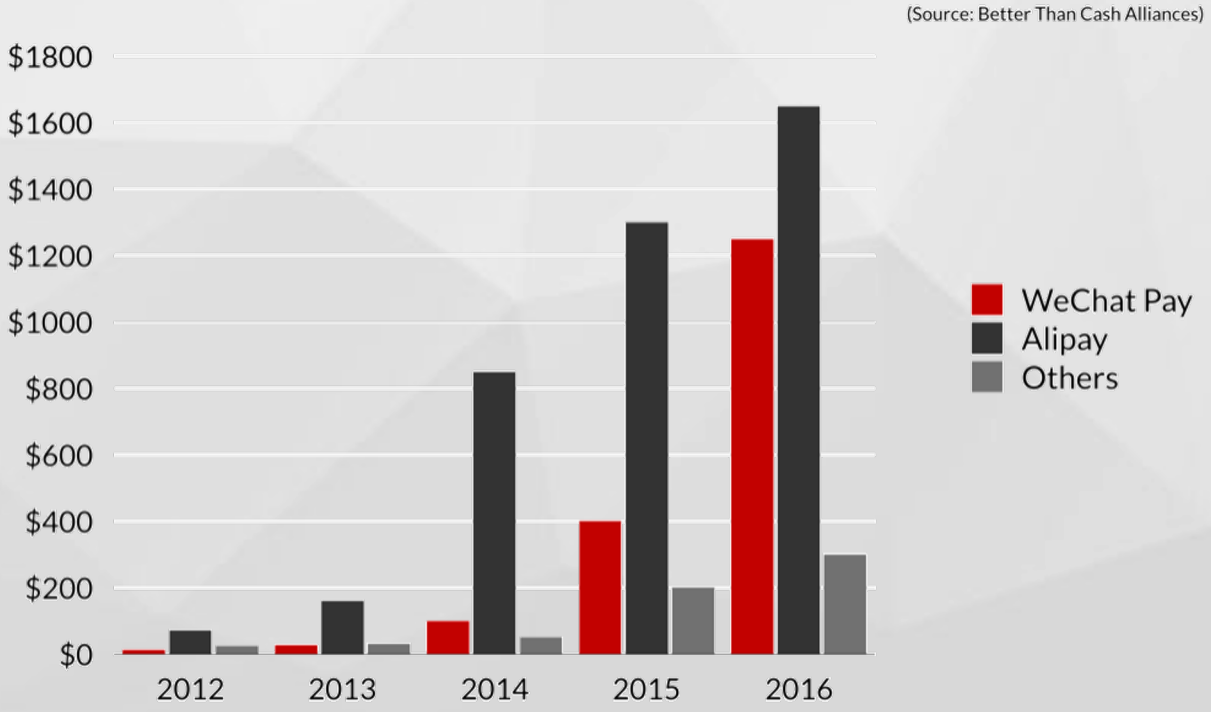

收付款
向商家付款
点击可查看付款码数字
零钱
优先使用此支付方式付款
二维码收款
赞赏码
Camera
Cashier

Growing up for Mobile Payments

How Many People in China Use Mobile Payments



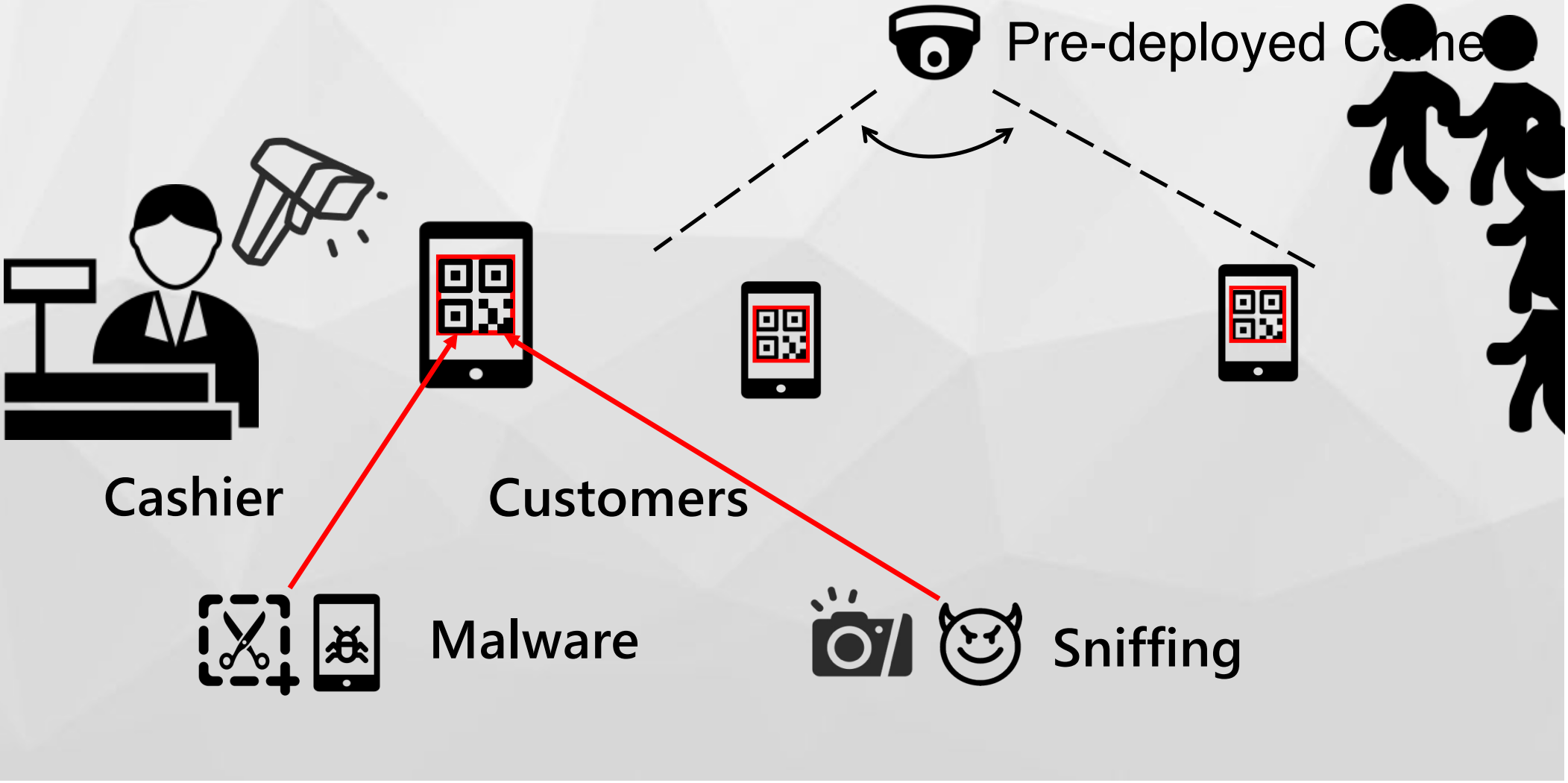
The growth of Mobile Payment by Value in China (Billon USD)



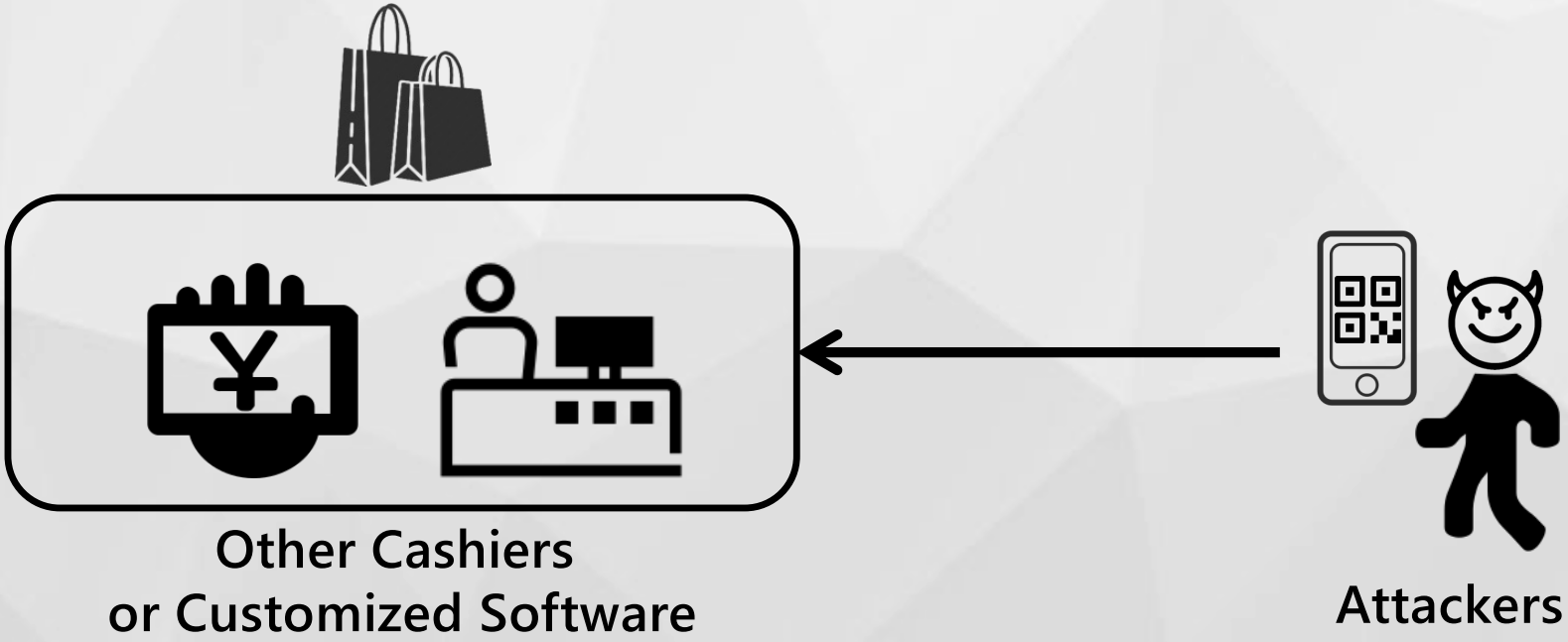
However

QR code is insecure...

Replay Attack in a Mobile Payment Scenario

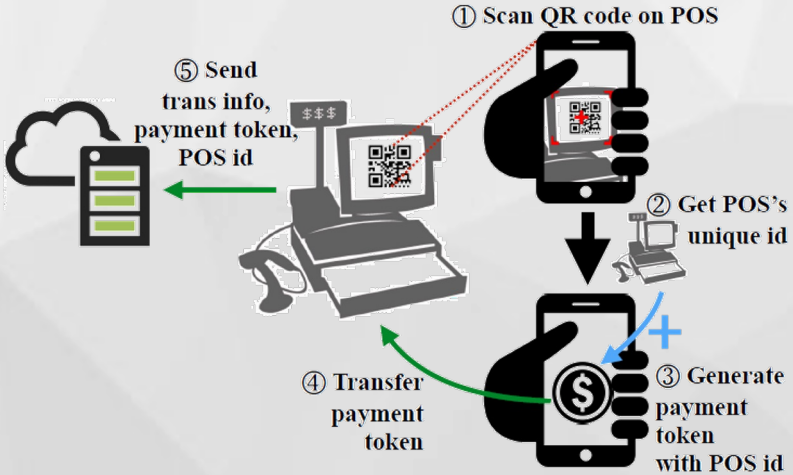


Replay Attack in a Mobile Payment Scenario



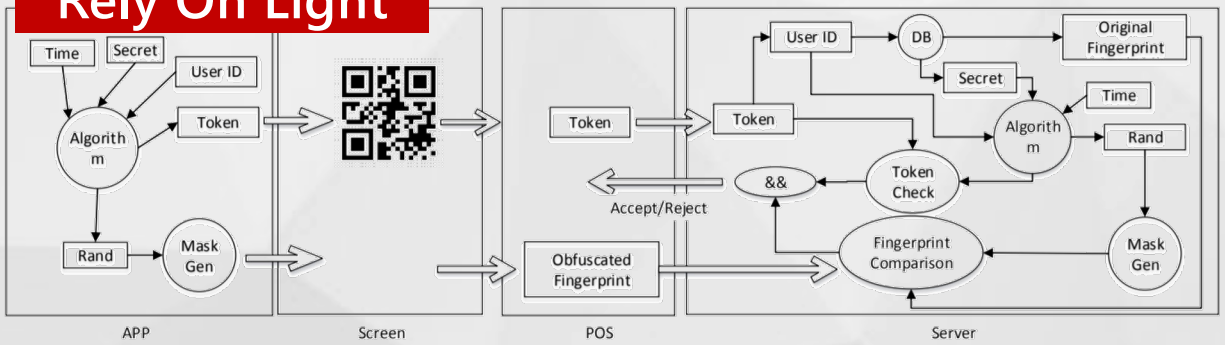
Existing Solutions

Change User's Habit



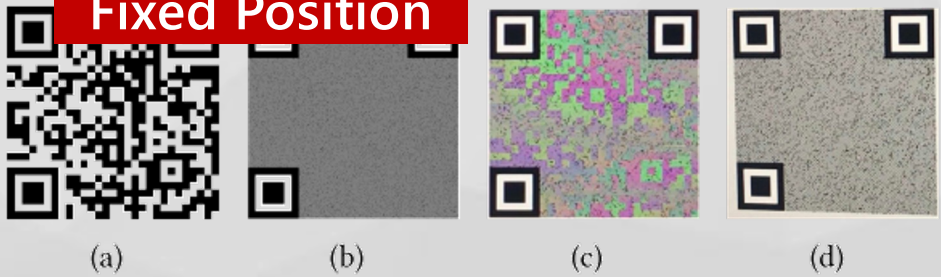
POSAUTH (USENIX 17')

Rely On Light



AnonPoint (ACSAC 18')

Fixed Position



mQRCode (Mobicom 19')


Hardware
Fingerprint
≠
Transaction
Denied!
Authorized
Phone
Attackers'
Phone
Cashier

PWM

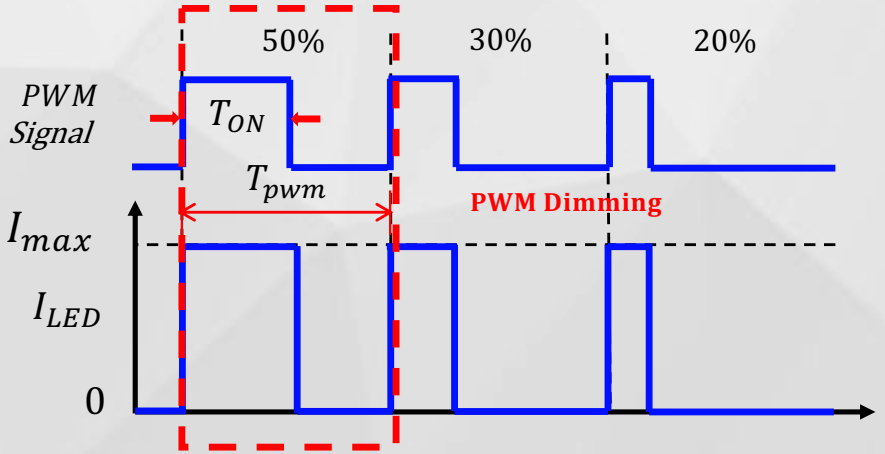
Frequency!

Working Principle of Pulse Width Modulation

Flicker

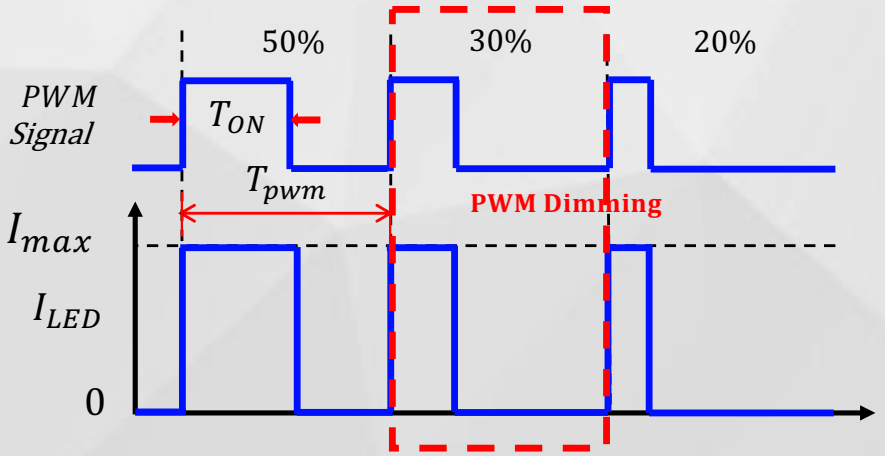
Brightness

Screen Brightness Control Using PWM



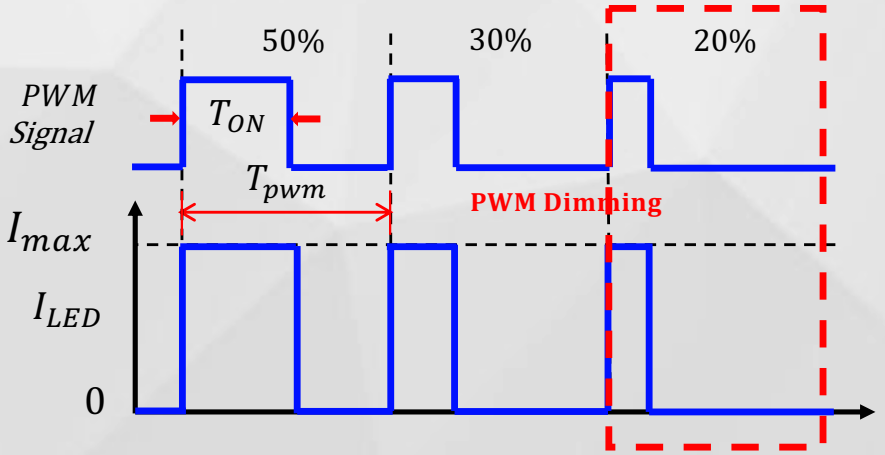
Working Principle of Pulse Width Modulation

Screen Brightness Control Using PWM



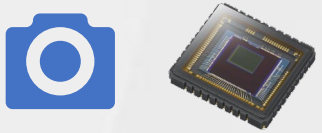
Working Principle of Pulse Width Modulation

Screen Brightness Control Using PWM

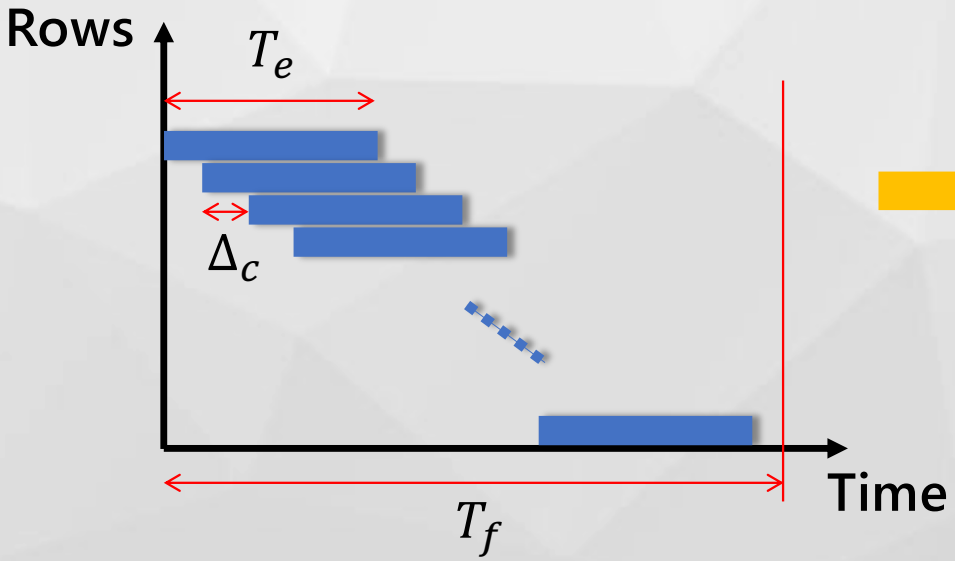


Communication Between Screen and Camera

Brightness control using PWM

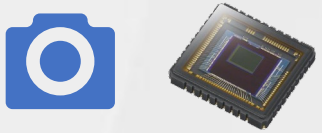


CMOS

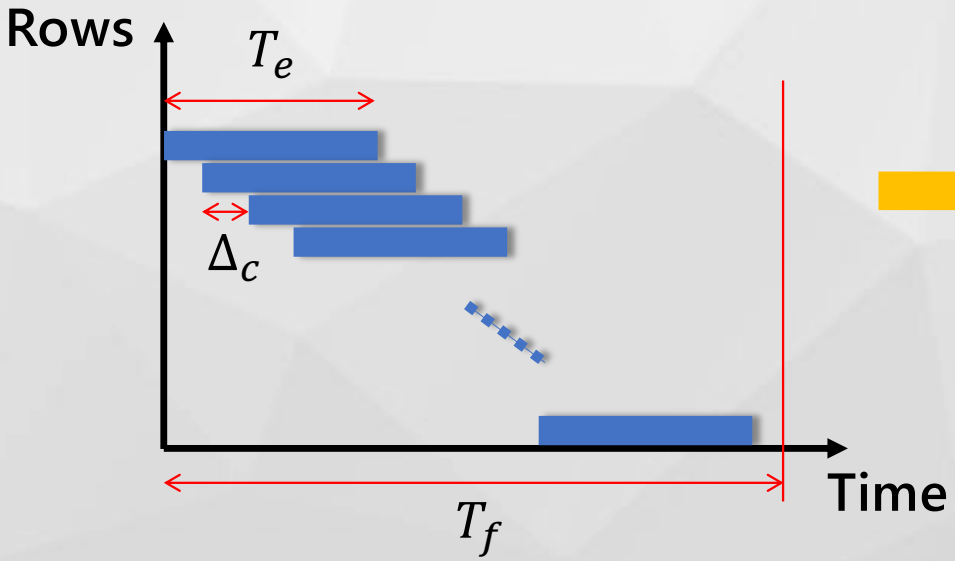


Communication Between Screen and Camera

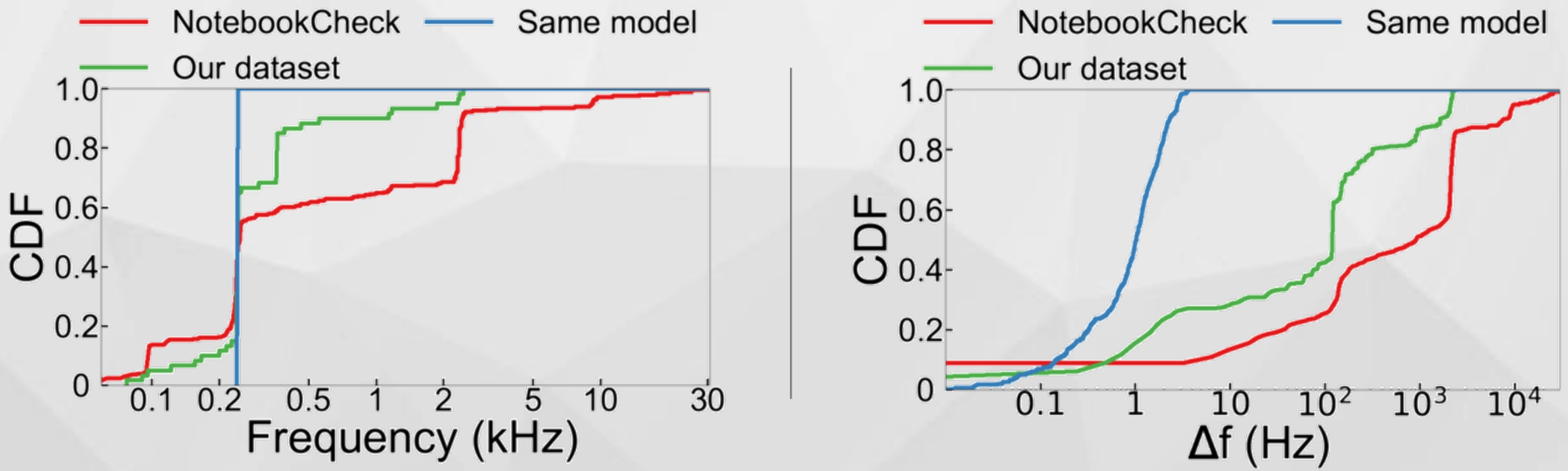
Brightness control using PWM



CMOS

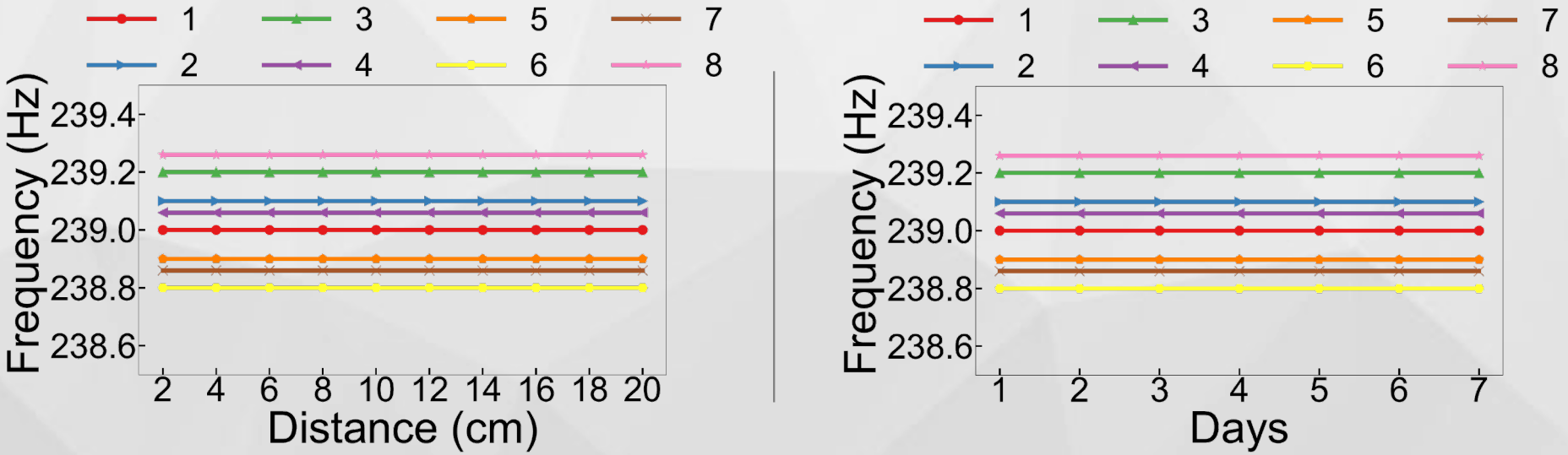


We select PWM frequency as fingerprint...



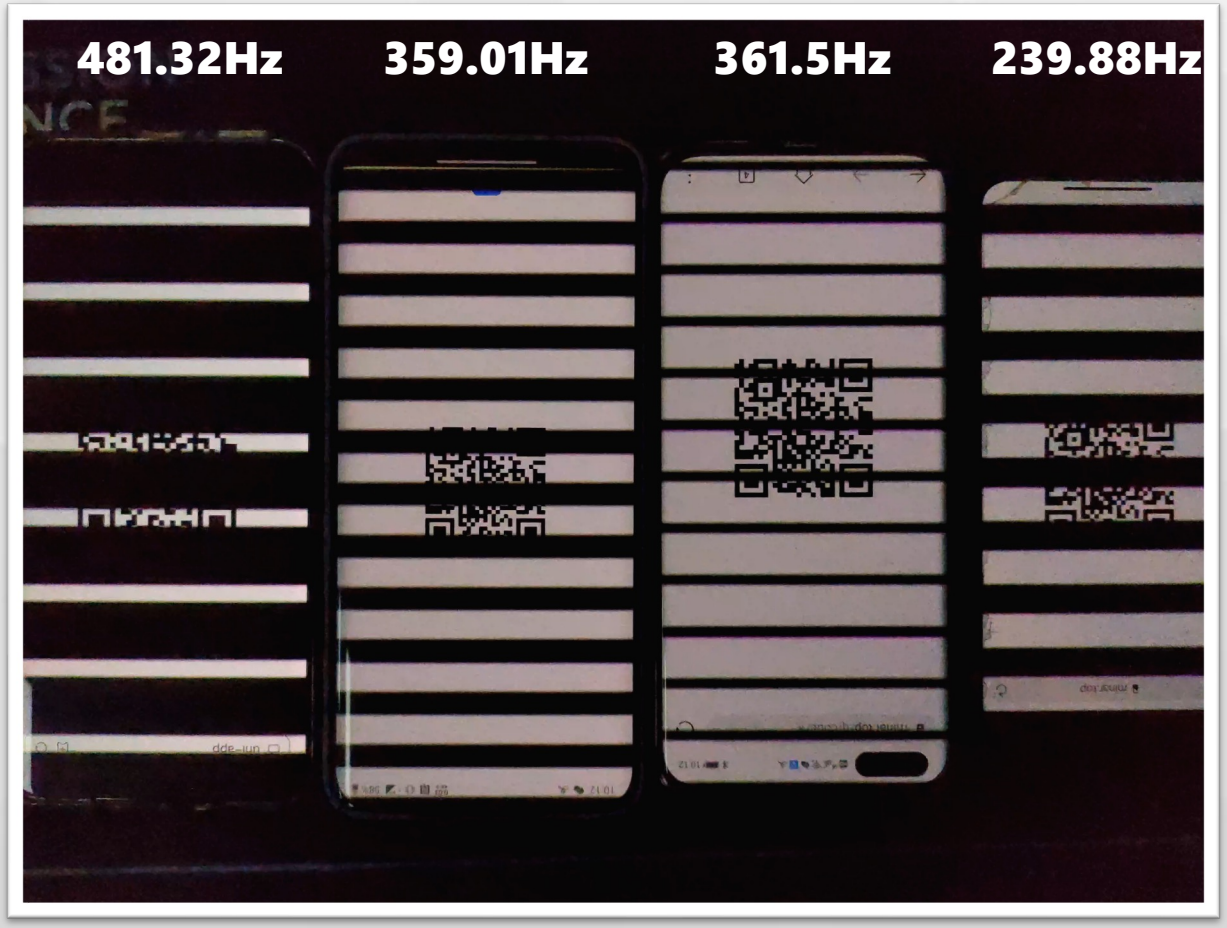
CDF of PWM frequencies and pairwise differences of 300 screens reported in NotebookCheck and 50 screens (16 are of the same model) we collected.

We select PWM frequency as fingerprint...



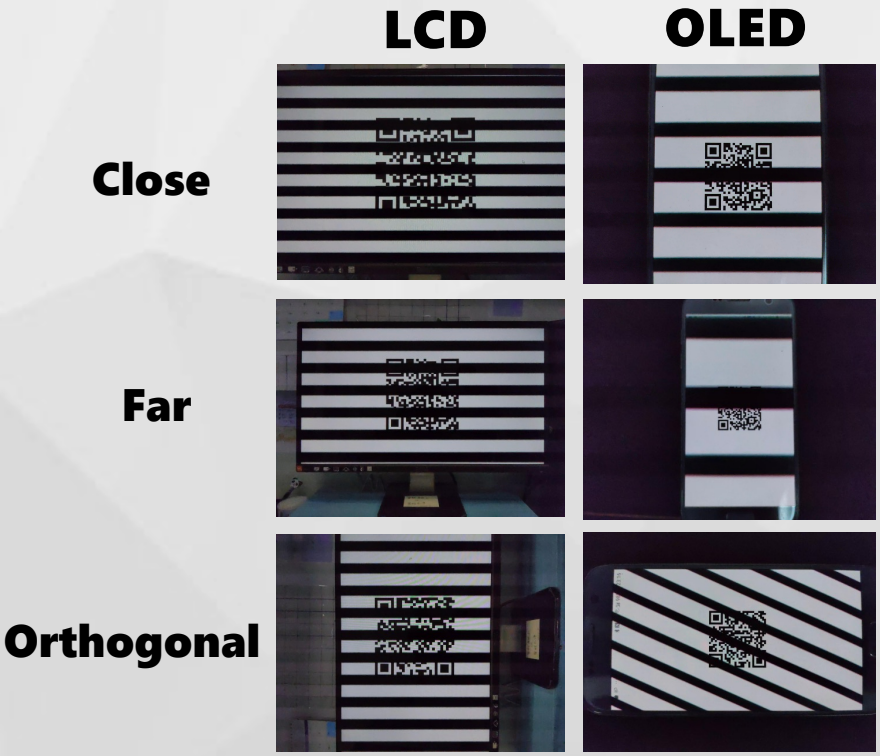
We measure the PWM frequencies using light sensor of 8 screens of the same model across days and at various distances to show its stability.

We select PWM frequency as fingerprint...



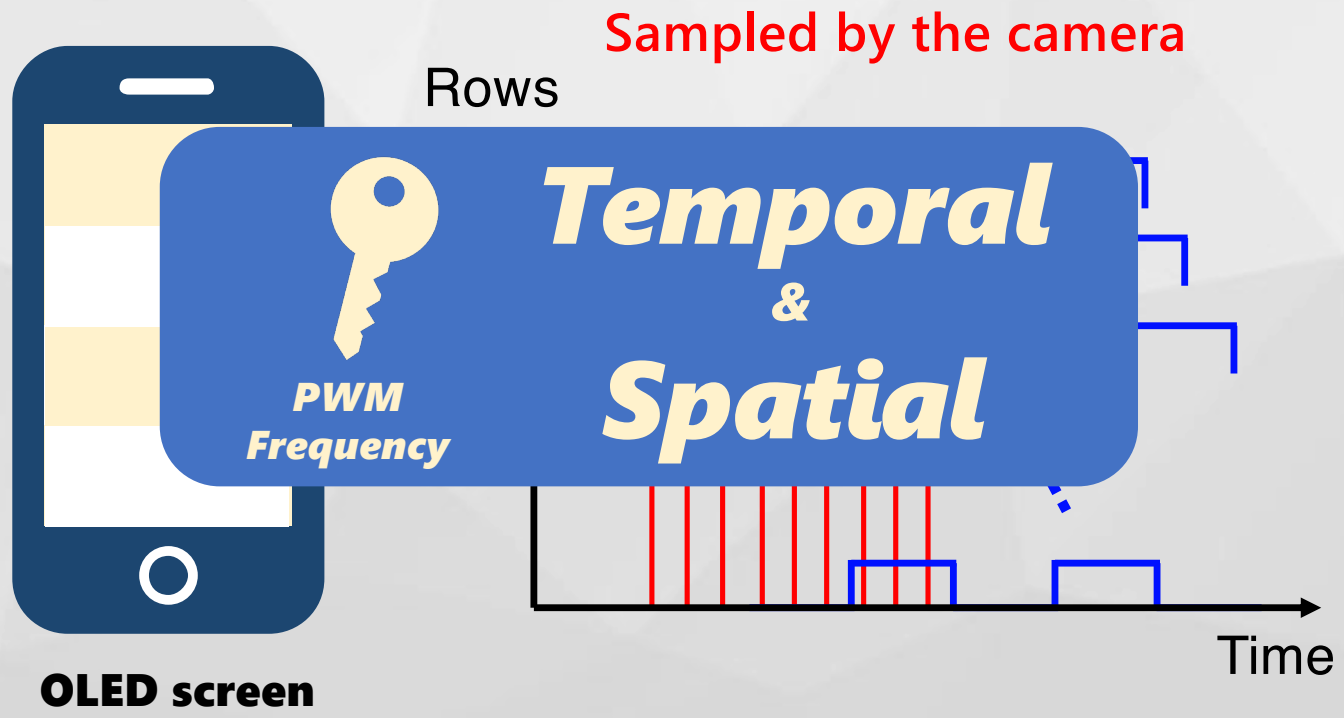
Challenge

Challenge 1

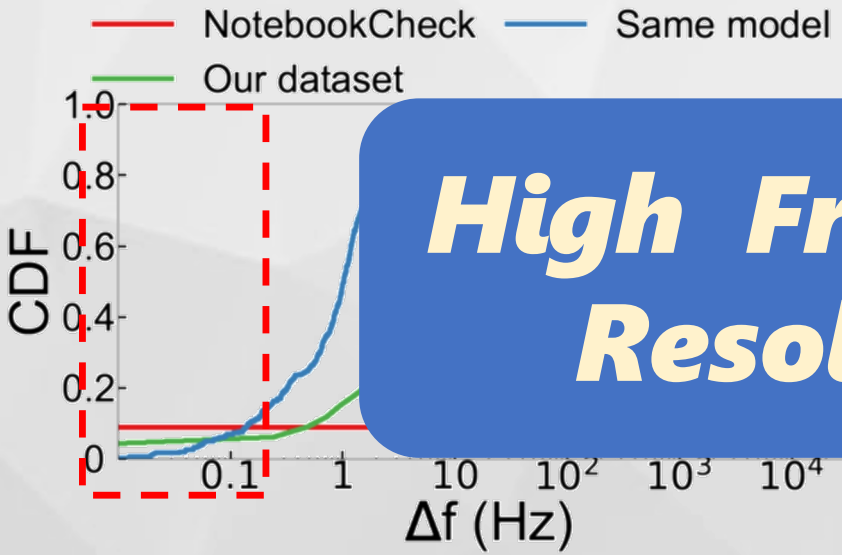

LCD
OLED
Close
Far
Orthogonal


Each row lights asynchronously
LCD screen
OLED screen

Challenge 2


Sampled by the camera
Rows
Temporal
&
Spatial
PWM
Frequency
Time
OLED screen

Challenge 3

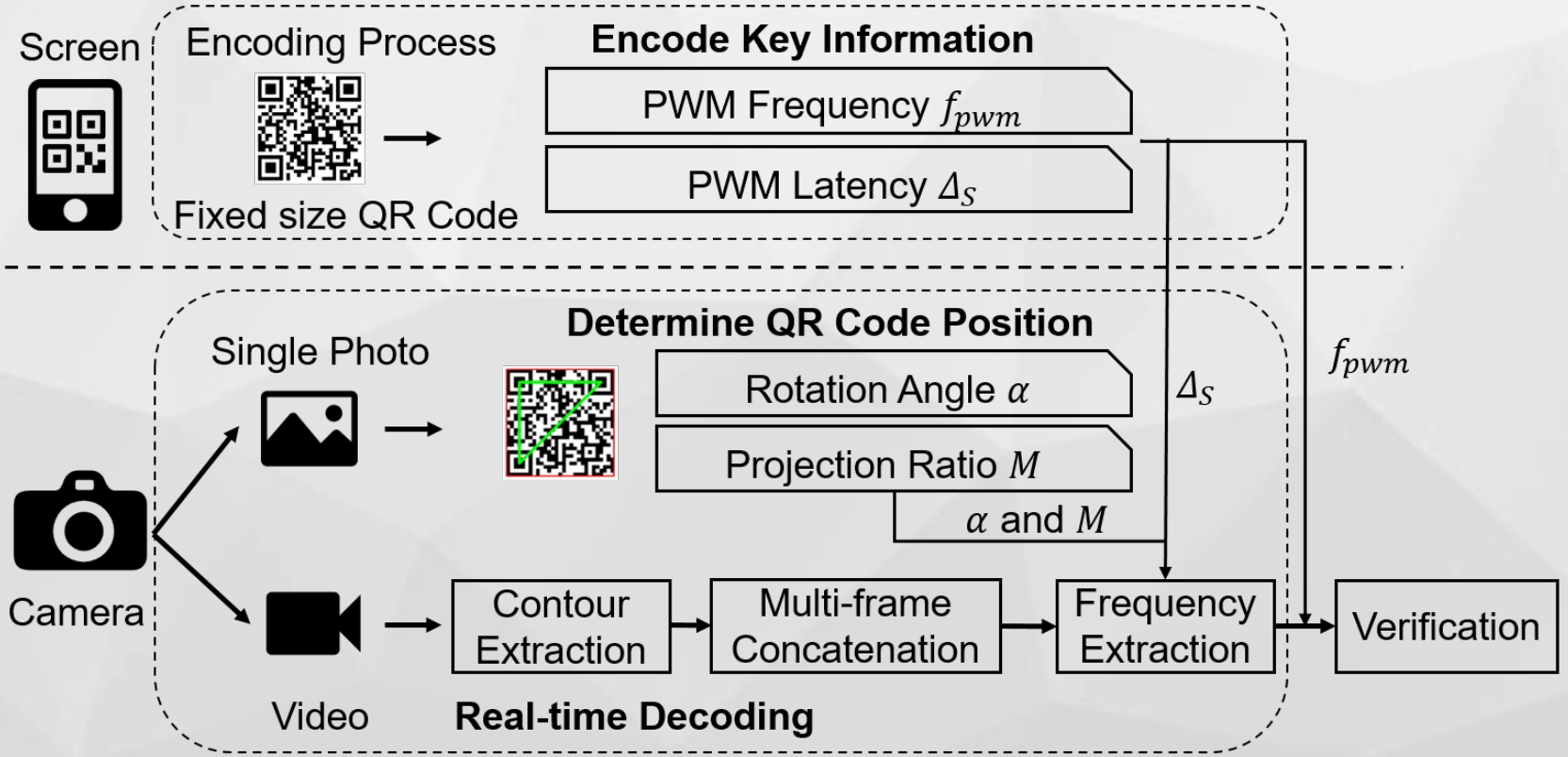


High Frequency Resolution

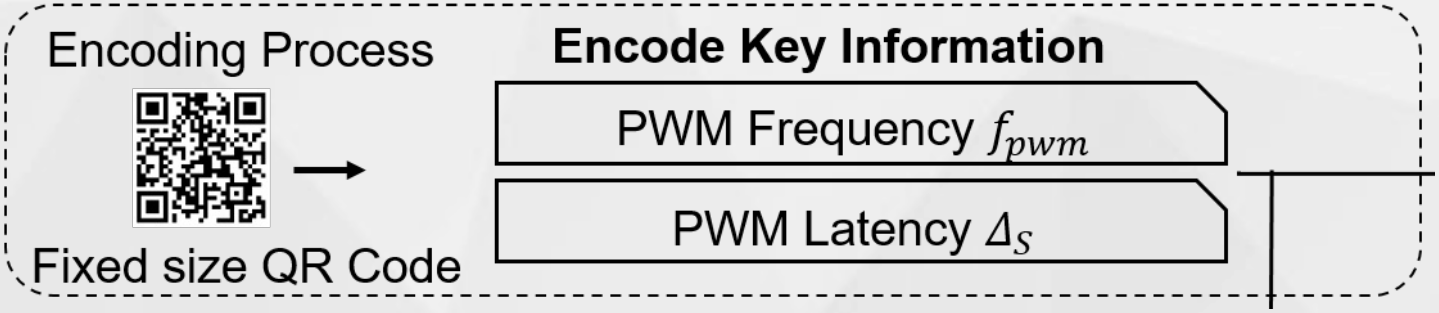
99.3% Screens

Pairwise differences of 300 screens

System Overview



System Overview



System Overview

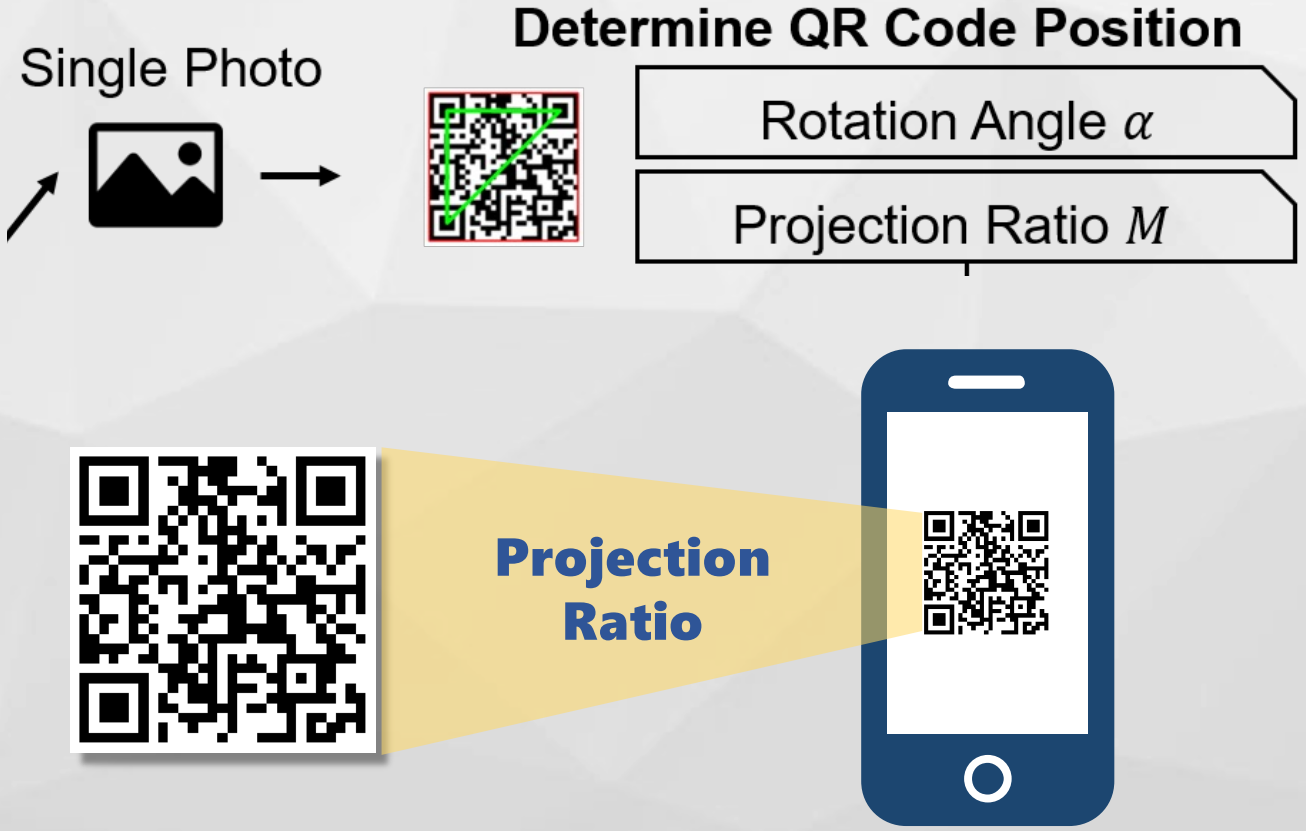
Single Photo

Determine QR Code Position

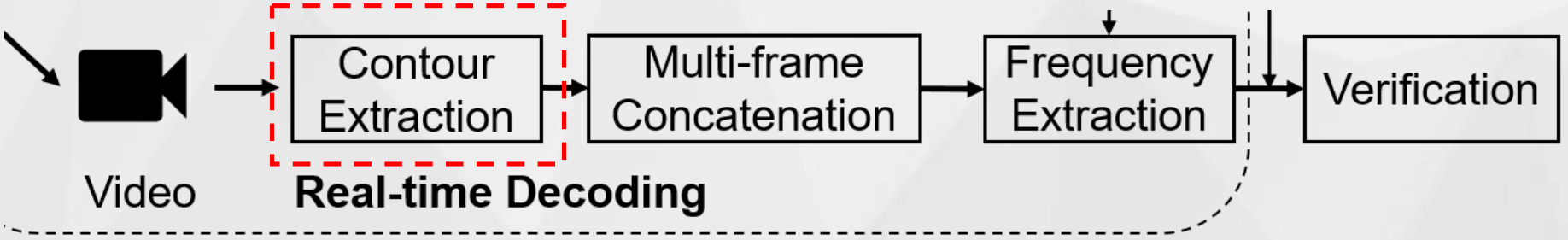
Rotation Angle α

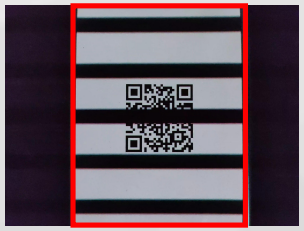
Projection Ratio M

System Overview

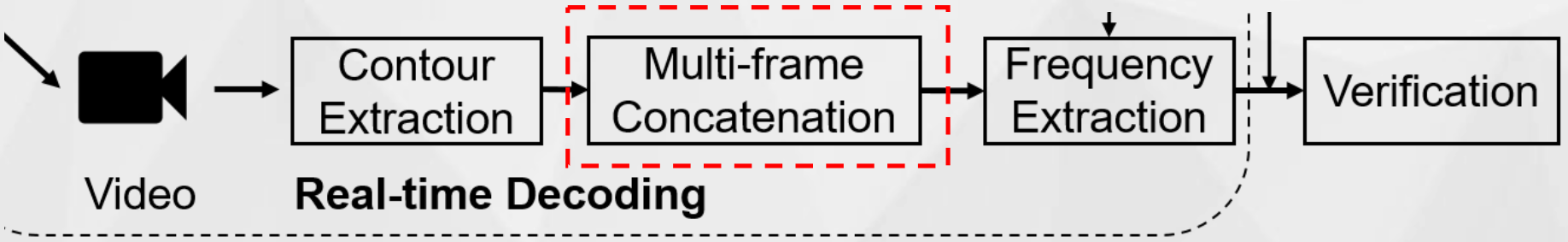


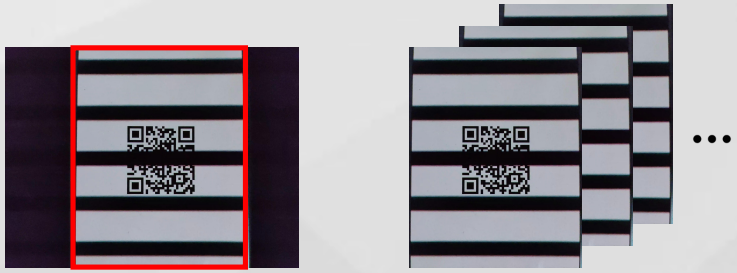
System Overview



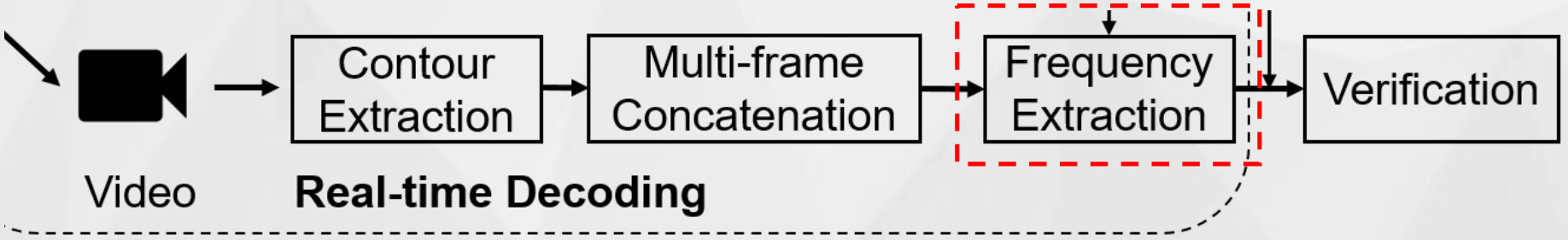


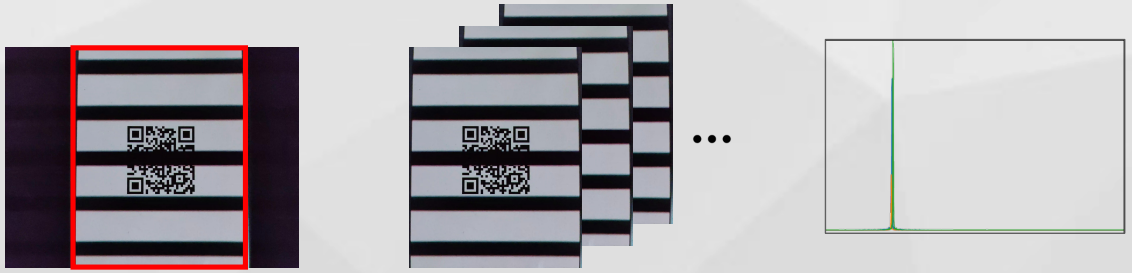
System Overview



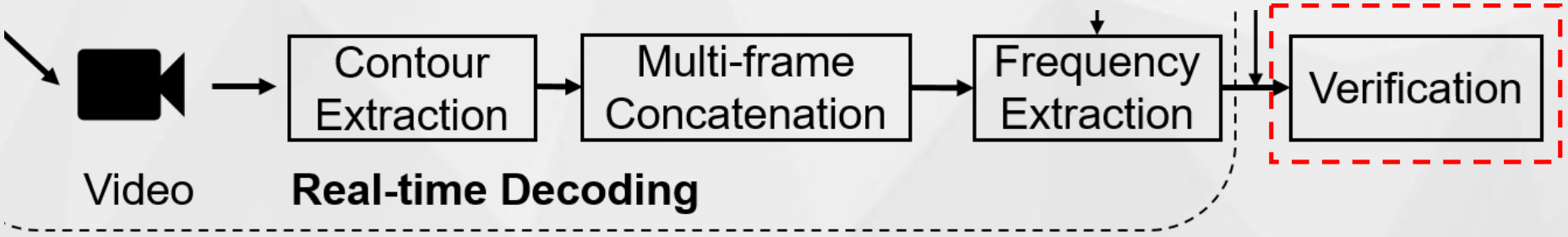


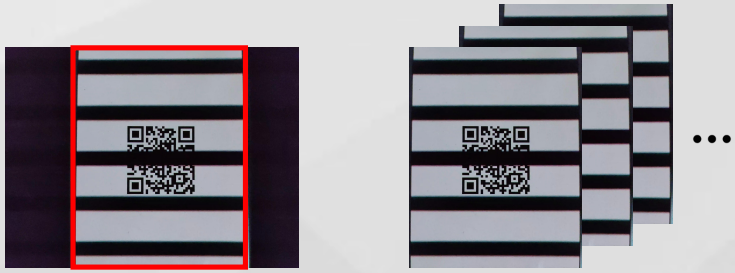
System Overview





System Overview





f_{pwm} ≠ ?

Performance Evaluation

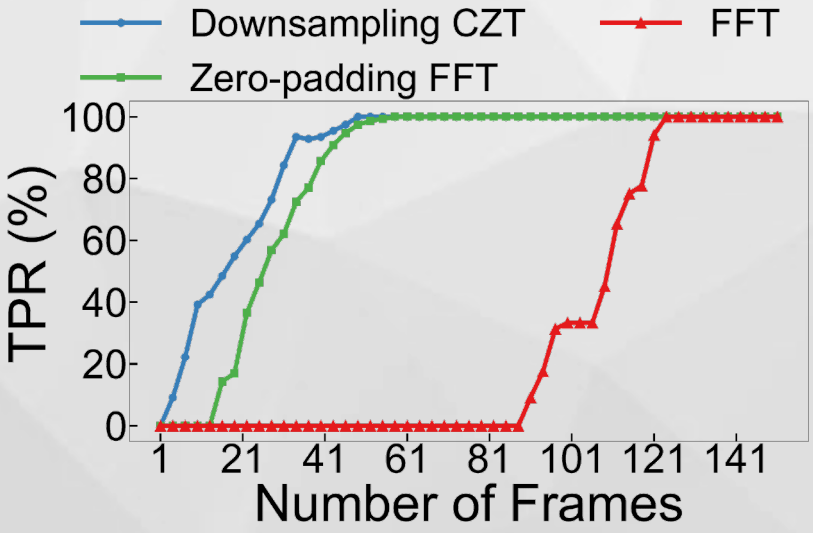
- Experiment Setup and Metrics:
  - We generate version-3 (29×29) QR codes using ScreenID. 50 smartphone screens (10 LCD and 40 OLED) and 5 smartphone cameras are used in our evaluation. We displayed 40 QR codes where 10 for verification and the other 30 selected randomly for attack.

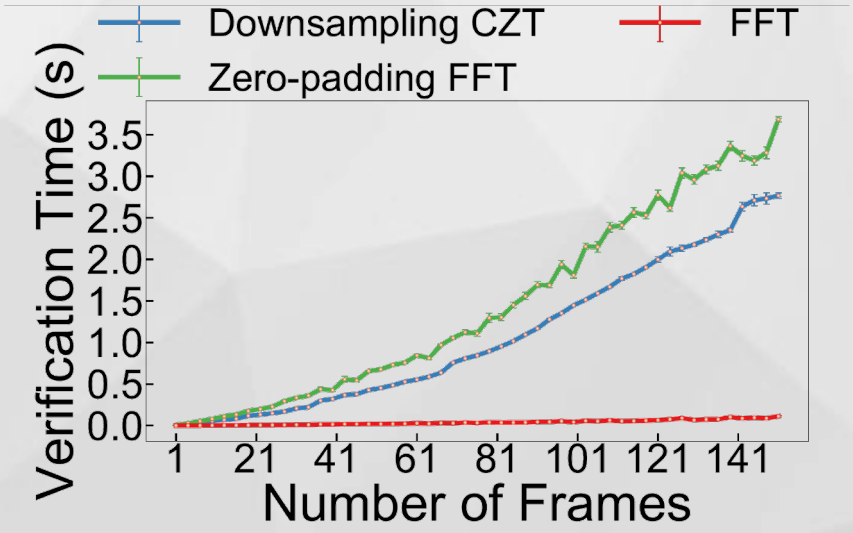
  - TPR (True Positive Rate) = $\frac{Number\ of\ accepted\ authorized\ QR\ code}{Number\ of\ verification\ attempts}$

    FPR (False Positive Rate) = $\frac{Number\ of\ accepted\ unauthorized\ QR\ code}{Number\ of\ attack\ attempts}$

Performance Evaluation - Microbenchmark

- Number of Required Frames

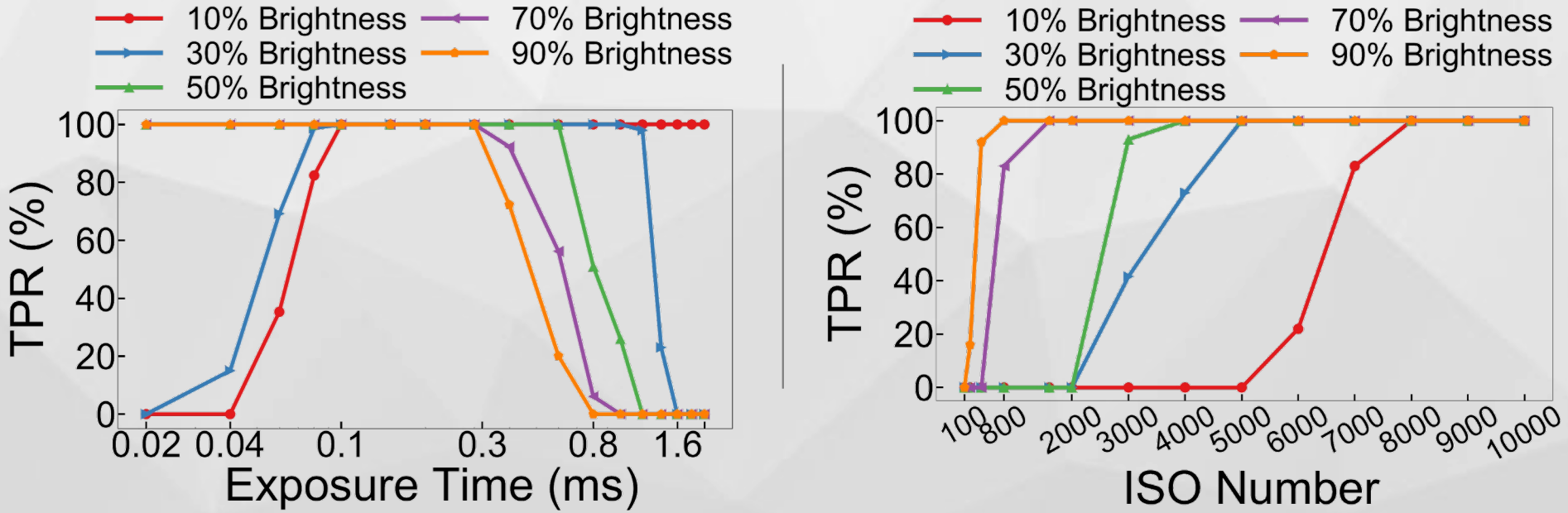




Verification TPR and time of different frequency extraction schemes.

Performance Evaluation - Microbenchmark

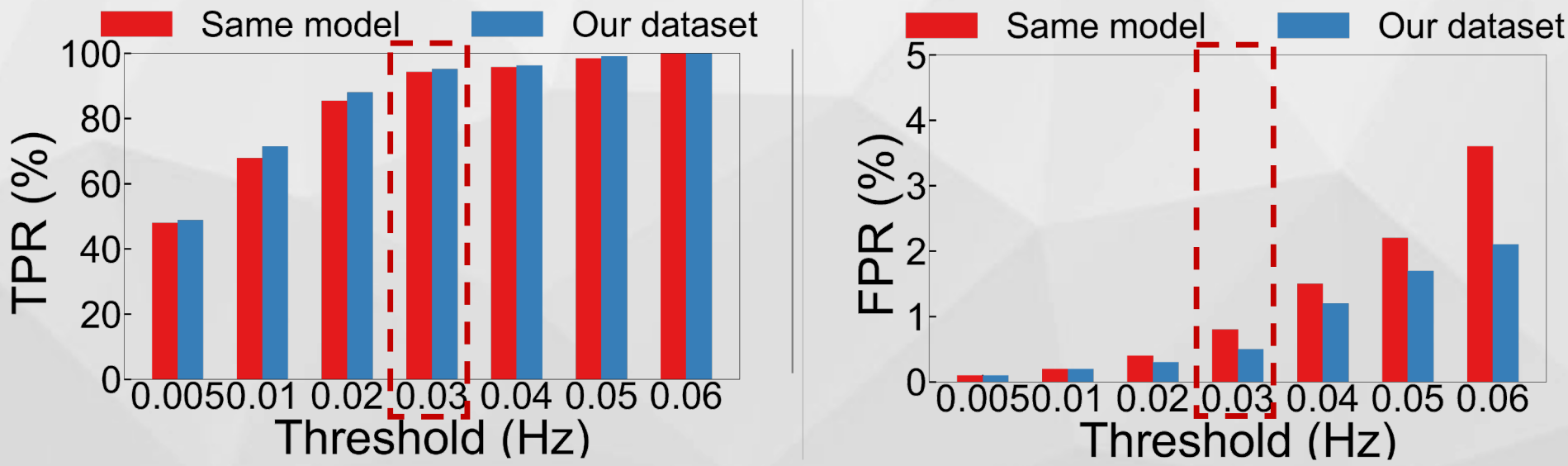
- Camera Configuration



The TPR on impact of exposure time and ISO number under different brightness ratio

Performance Evaluation - Microbenchmark

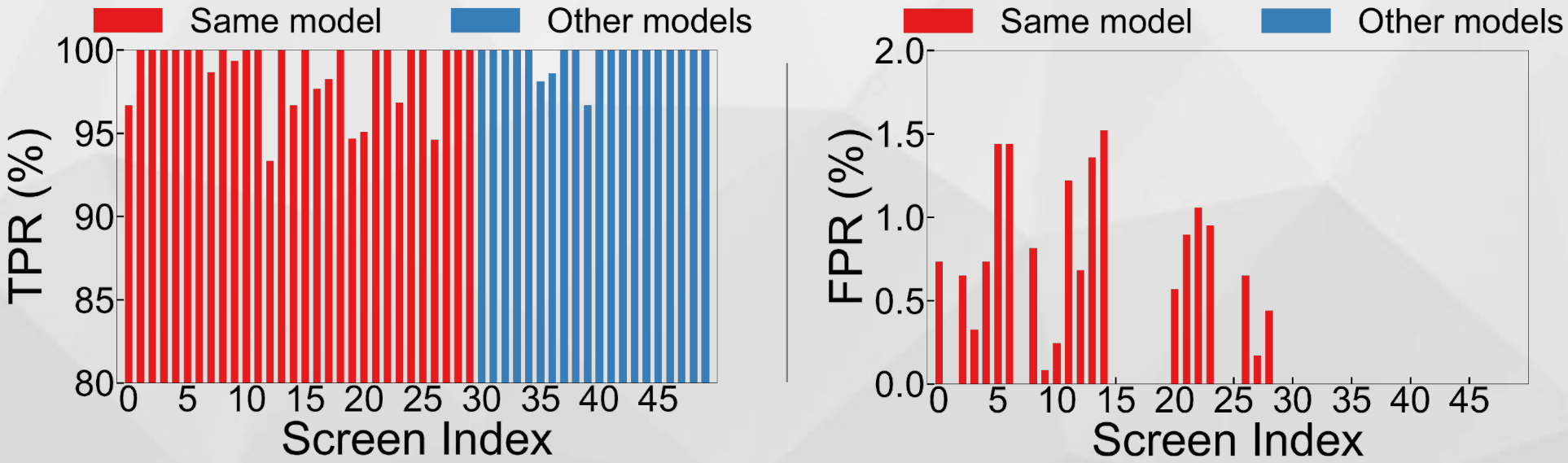
- Threshold



The TPR and FPR on the impact of 50 screens we collected

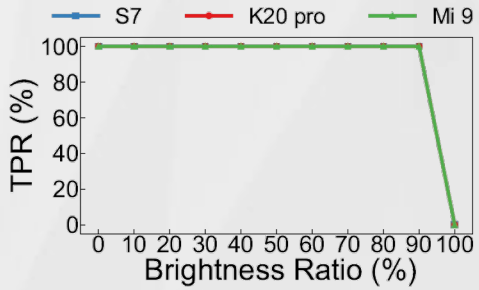
Performance Evaluation

- Overall Performance

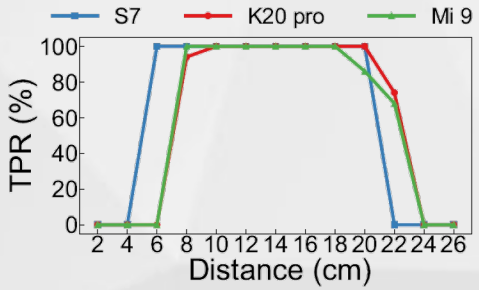


The TPR and FPR of 50 screens where the first 30(red) are of the same model

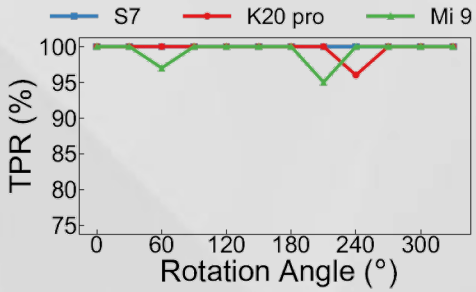
Performance Evaluation - Robustness



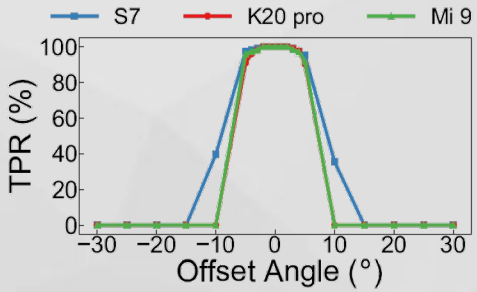
(a) Impact of screen brightness.



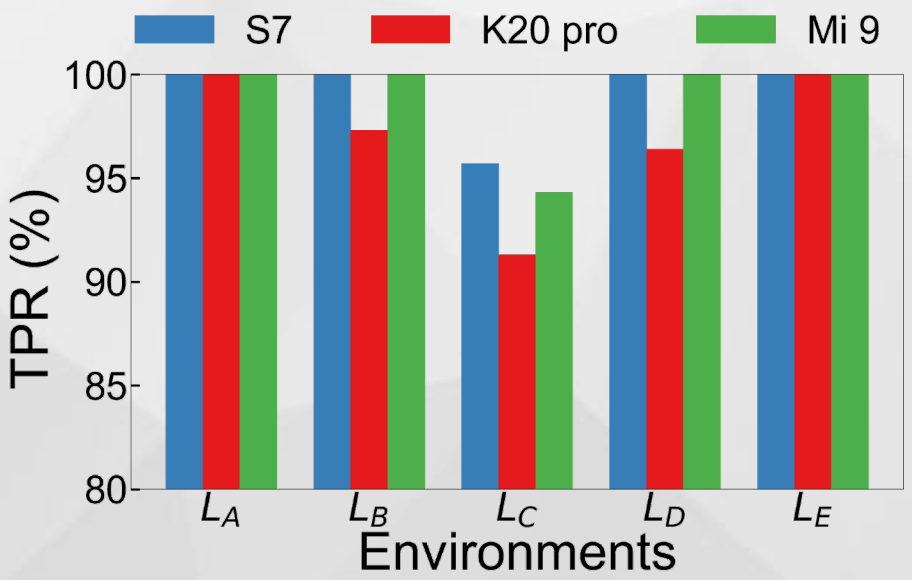
(b) Impact of capture distance.



(c) Impact of rotation angle.



(d) Impact of offset angle.



L_A: indoor with light off
L_B, L_C, L_D: outdoor at 9am, 12am, 5pm
L_E: indoor with light on

The robustness of ScreenID under various impact factors.

Conclusion

- We demonstrated the feasibility of using PWM frequency of screens for fingerprint, which can enhance QR code security.
- We proposed ScreenID, which incurs no additional hardware for QRCode system and no requirements for user behavior.
- We proposed to model the interaction between the camera and the screen in both temporal and spatial domains and achieved high estimation accuracy.
- We conducted exhaustive experiments and demonstrated the efficacy of ScreenID system under a variety of operating conditions.

Thanks

For Watching!