IEEE INFOCOM

Effectively Learning Moiré QR Code Decryption from Simulated Data

Yu Lu[†], Hao Pan[†*], Feitong Tan[‡], Yi-Chao Chen[†],

Jiadi Yu[†], Jinghai He[♦], Guangtao Xue[†*]

Shanghai Jiao Tong University [†]

Simon Fraser University [‡]

University of California, Berkeley [♦]

SHANGHAI JIAO TONG UNIVERSITY

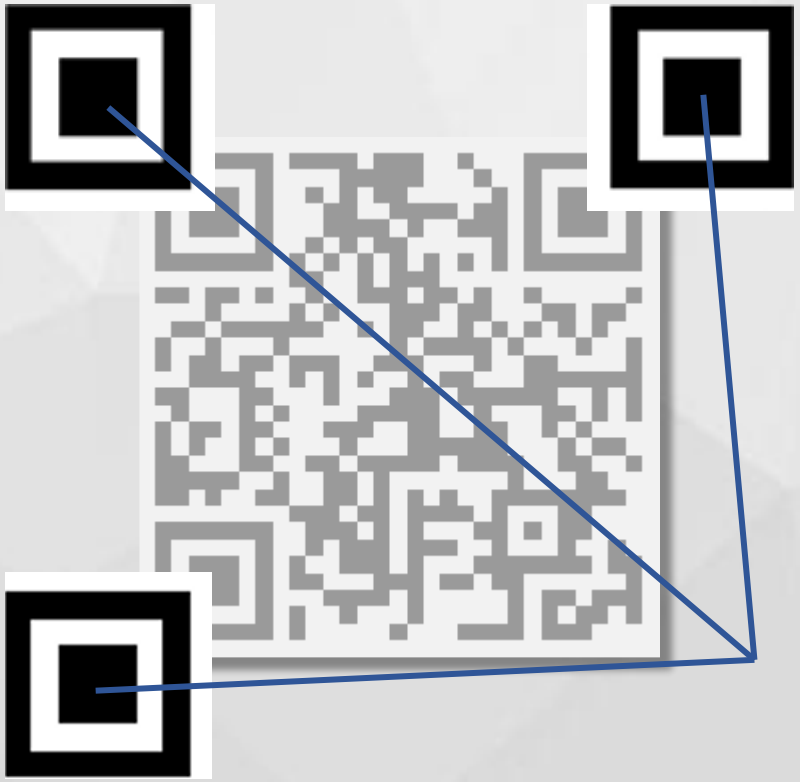
SFU SIMON FRASER UNIVERSITY

Berkeley UNIVERSITY OF CALIFORNIA

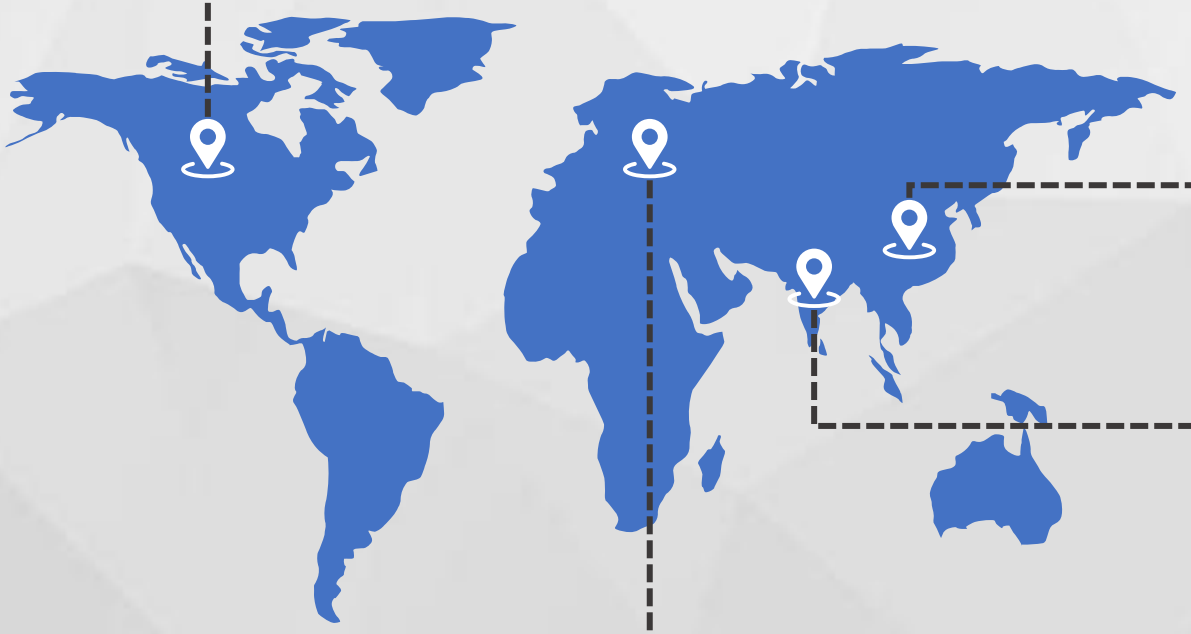
QR Code

Q R Code

Quick Response Code



Position Markers



In 2021, 75.8 million users in the US scanned a QR Code on their mobile.

The QR Codes payments now account for over 90% of China's mobile payments.

As of October 2021, the usage of the Bharat QR Code grew above 4.5 million in India.

75% of consumers have scanned a QR Code on FMCG products.

QR Code has become popular!

QR Code has become popular!

Payment

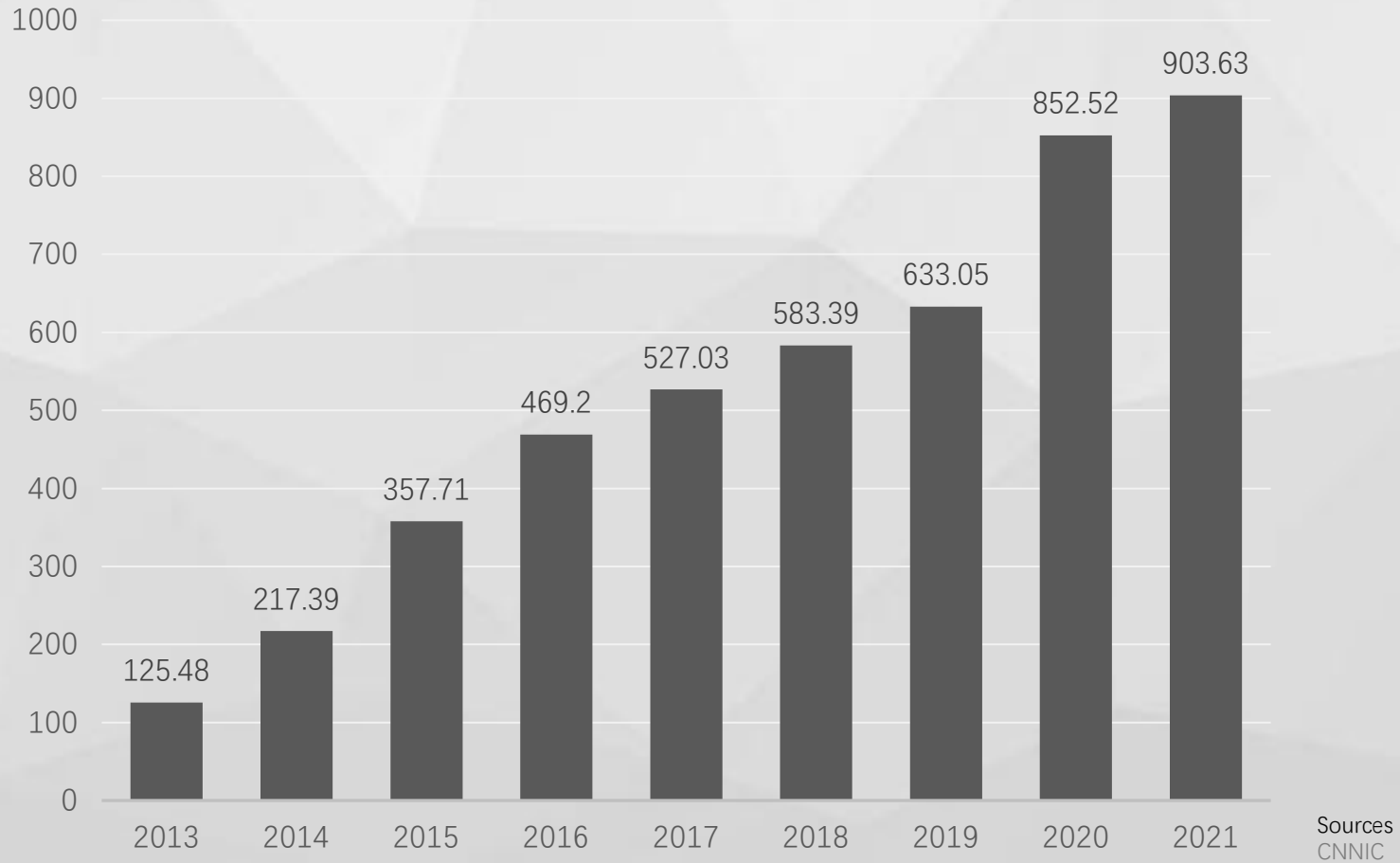
Advertisements

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

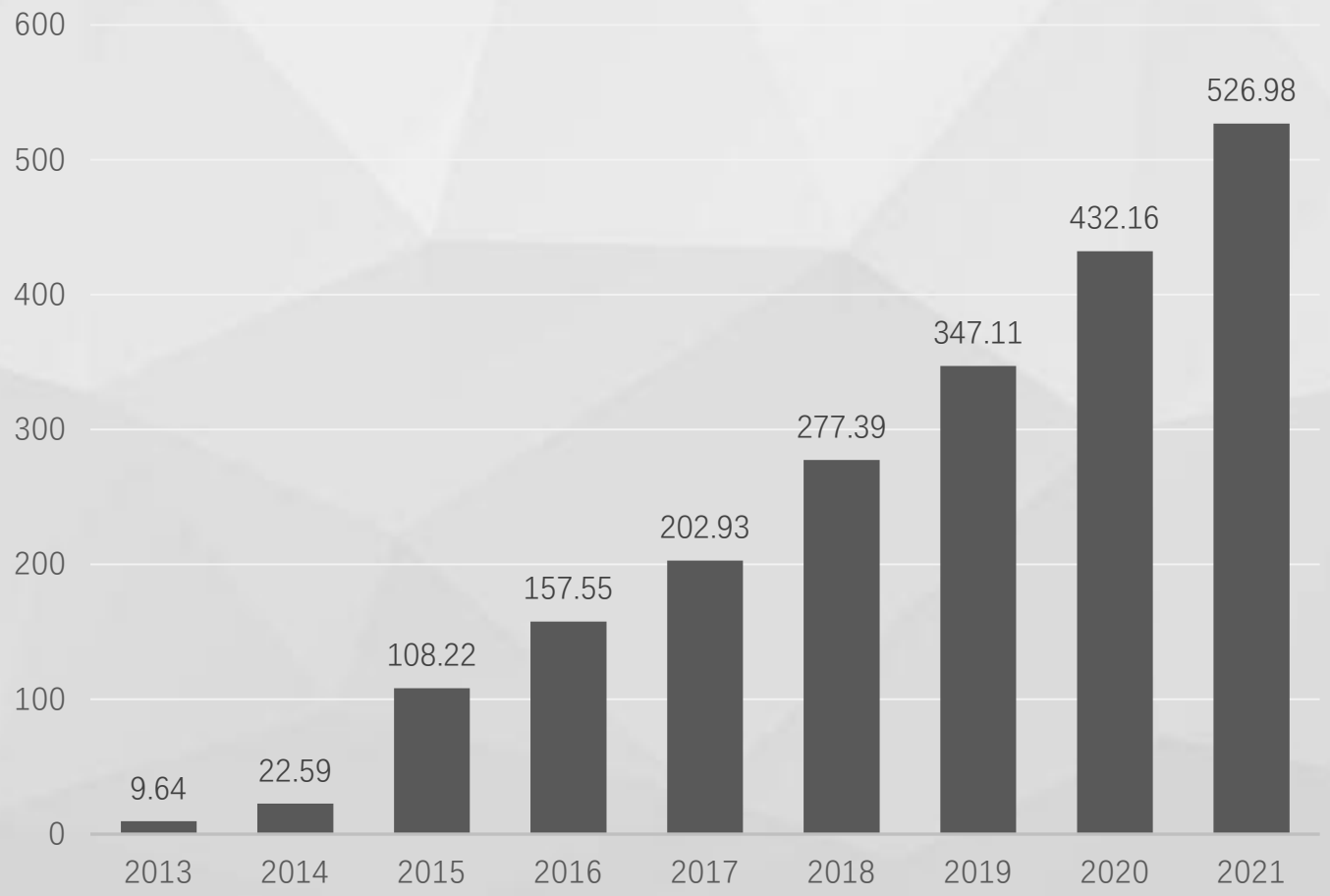
How Many People in China Use Mobile Payments (million)



Sources
CNNIC

Growing up for Mobile Payments

The growth of Mobile Payment by Value in China (Trillion yuan)

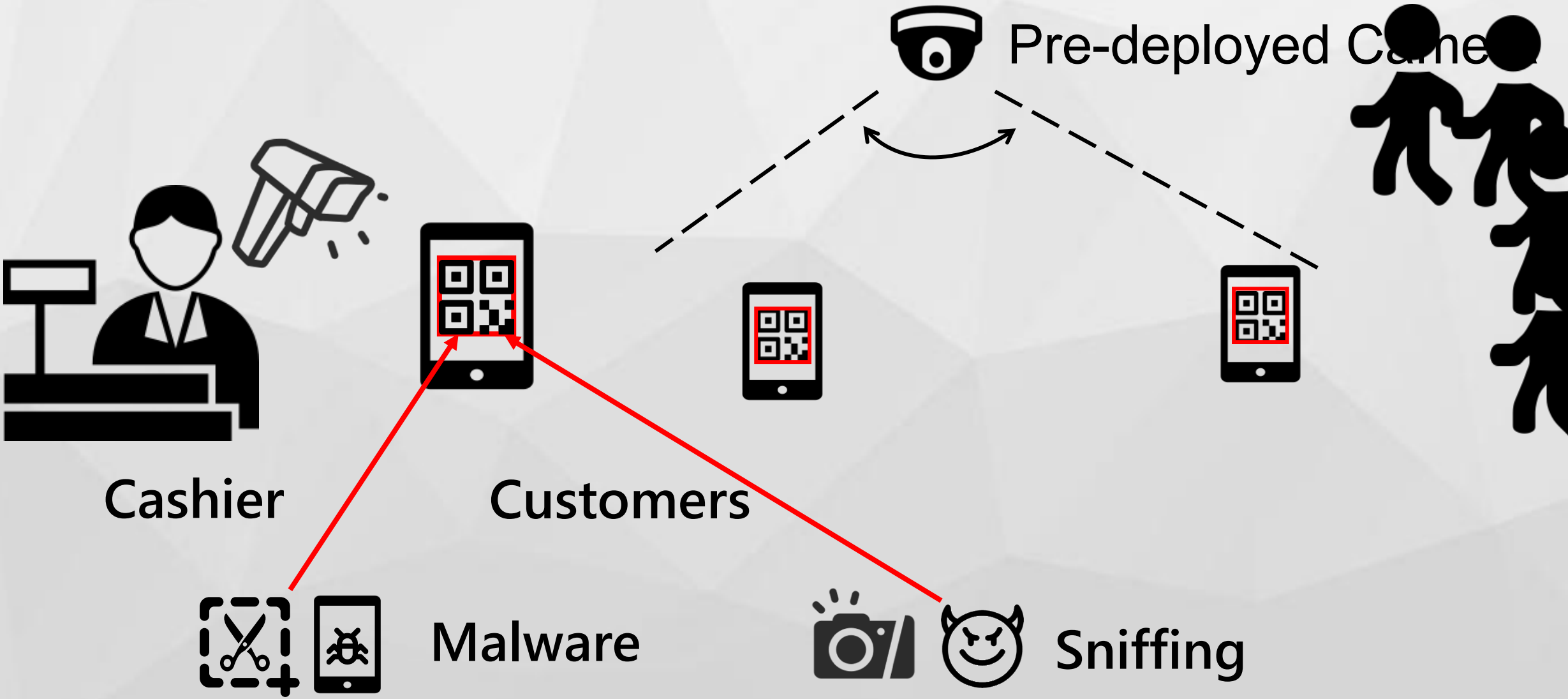


Sources
State Administration of Foreign Exchange;
People´s Bank of China

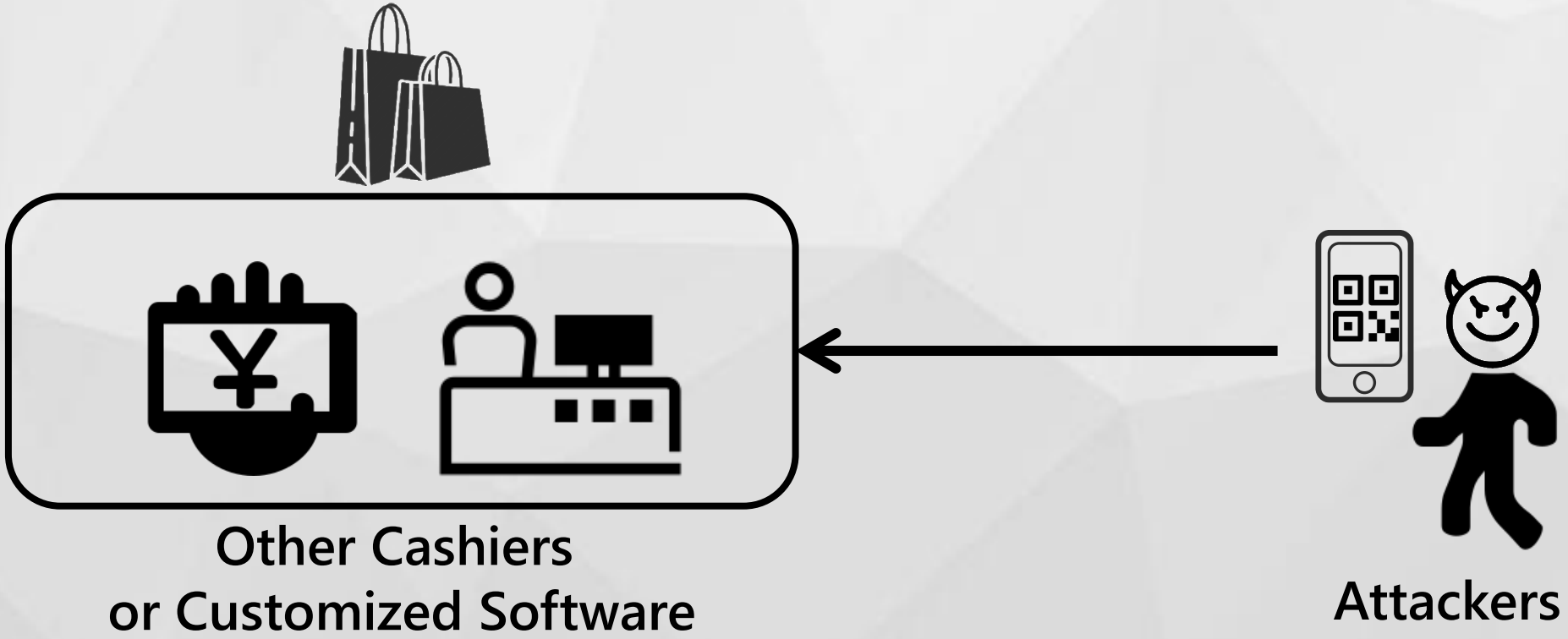
However

QR code is insecure…

Replay Attack in a Mobile Payment Scenario



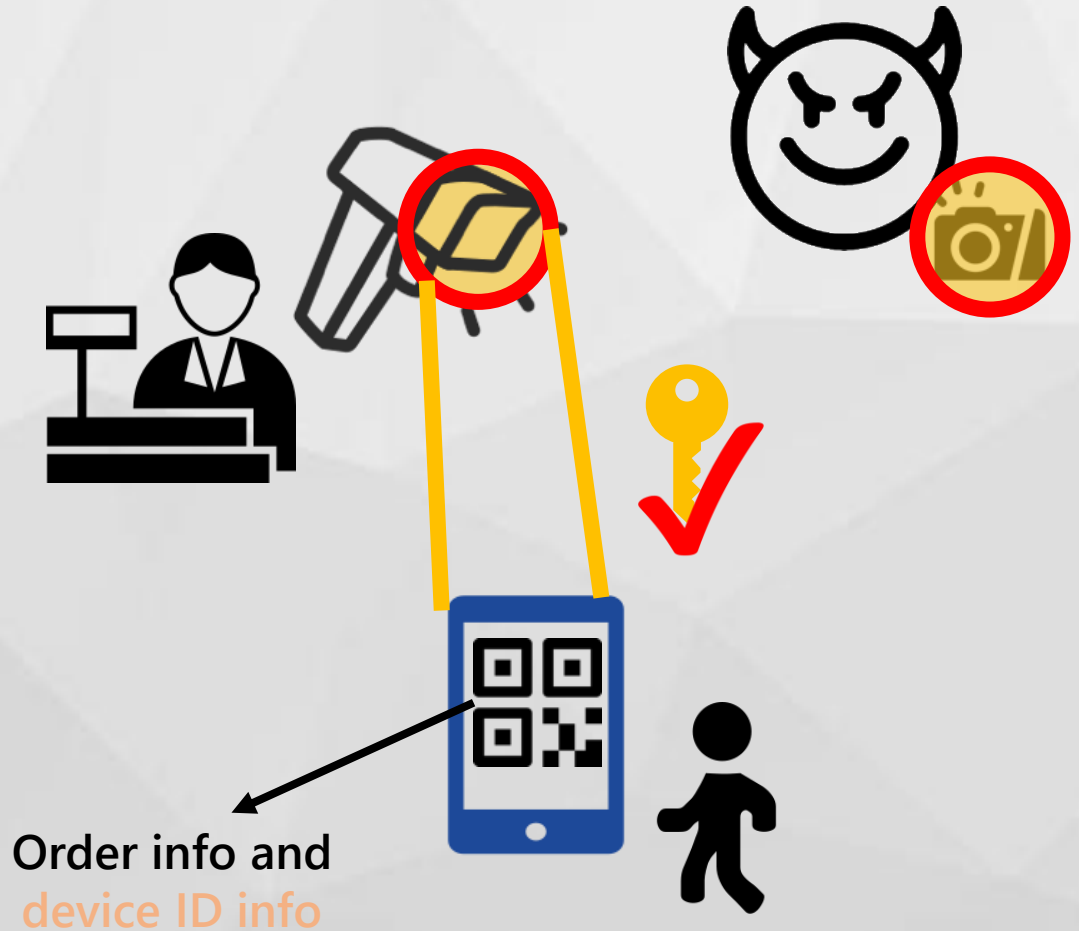
Replay Attack in a Mobile Payment Scenario

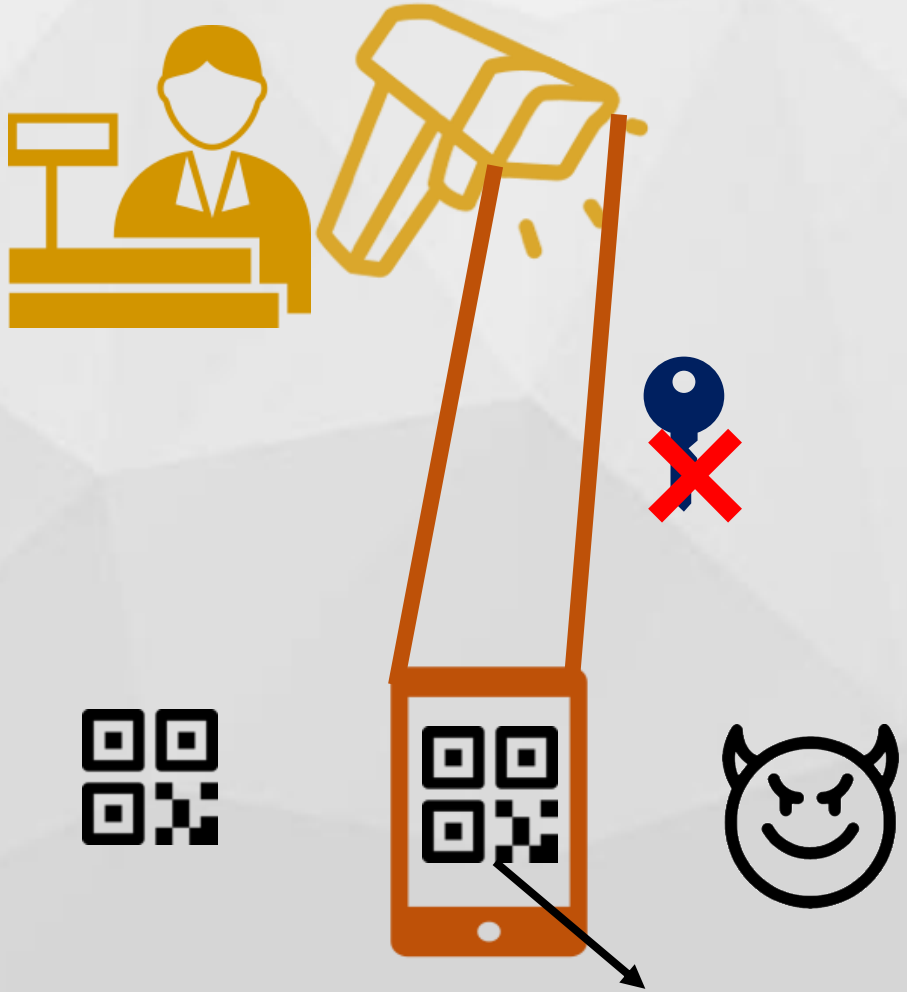


Why are QR codes vulnerable to replay attacks?

- ☐ It is a visible light communication
- ☐ It is a one-way communication

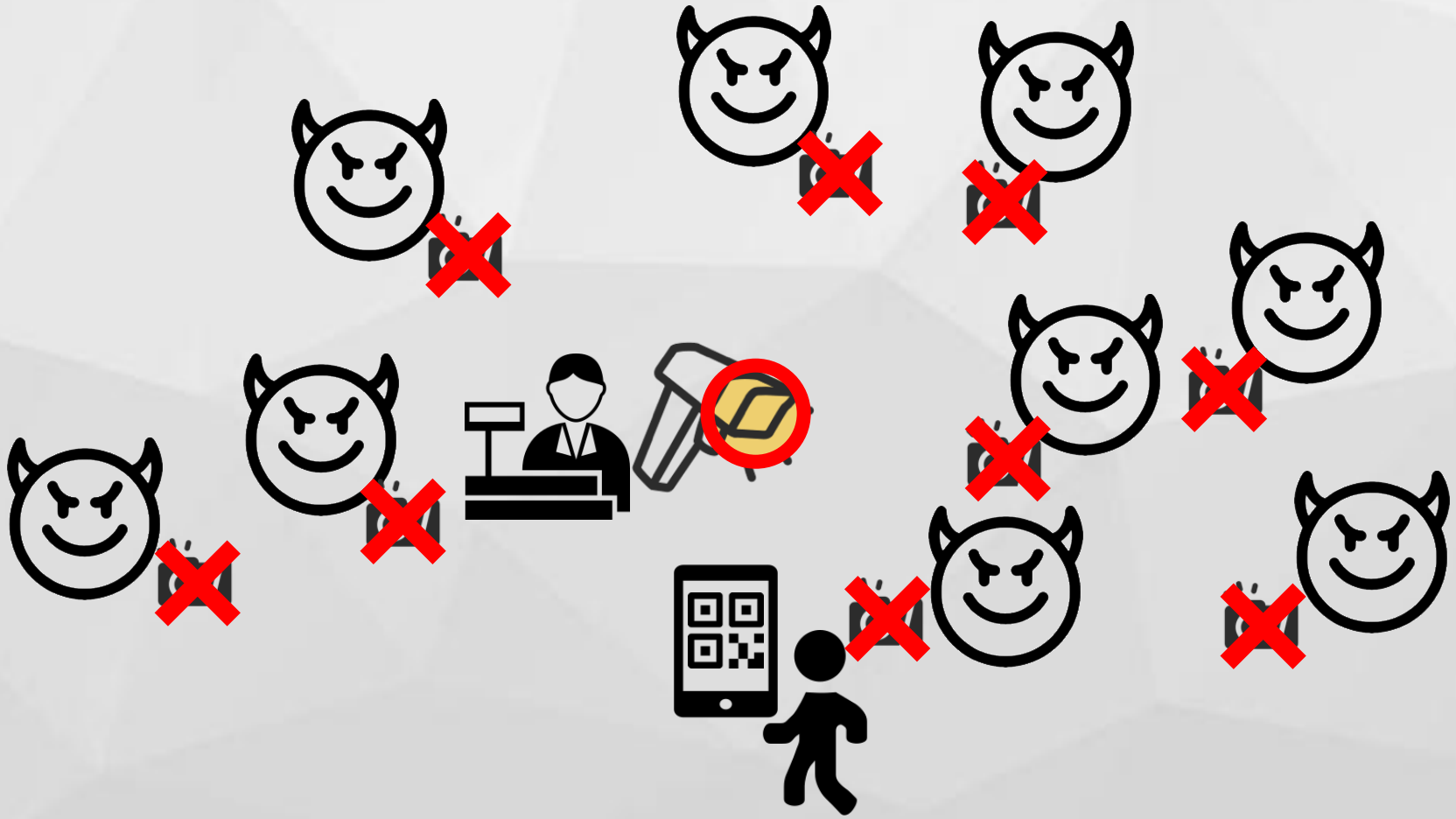
Related work: Add hardware info to realize authentication





Add the device ID information

Can we add the security of the screen-camera channel?

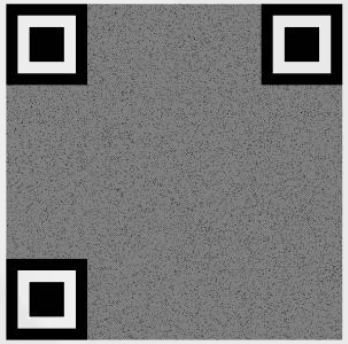


Reduce reception range

Nonlinearity of Spatial Frequency in Light !

Solutions: Moiré QR Code

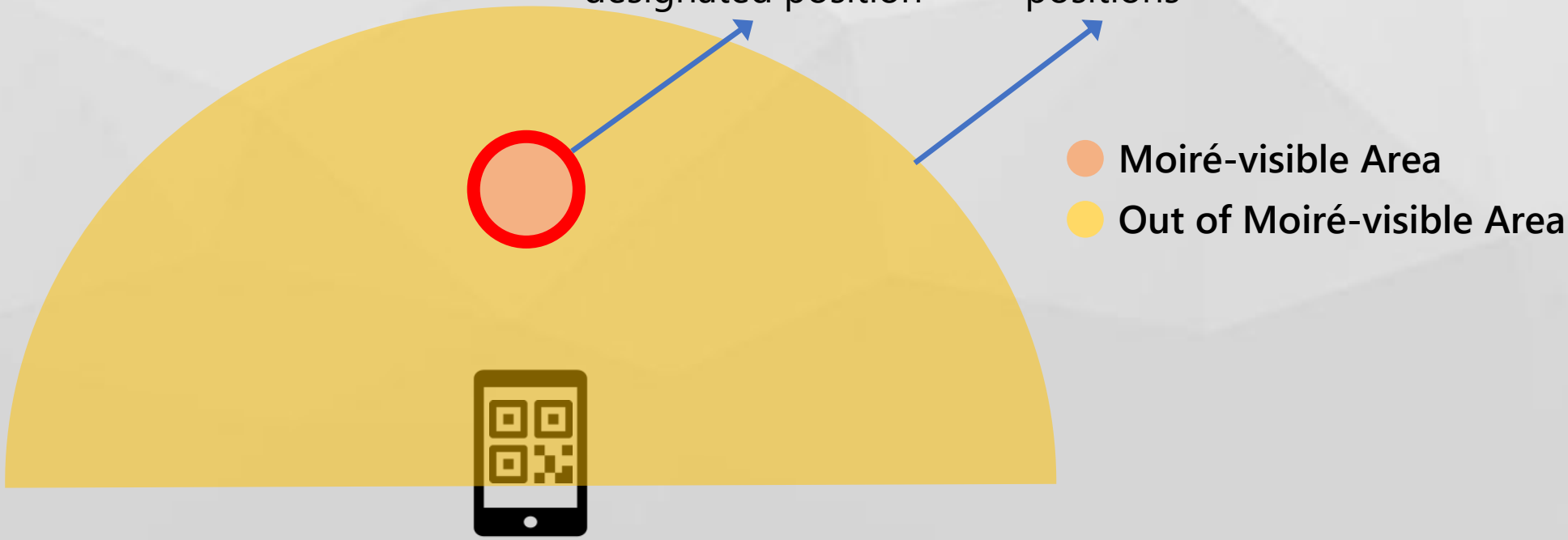
QR code



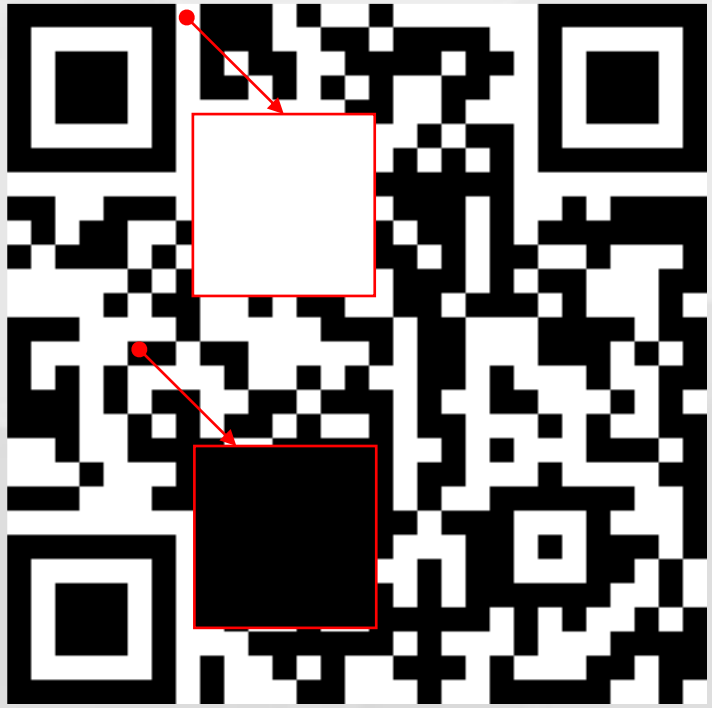
Moiré QR Code

Photographs taken at the designated position

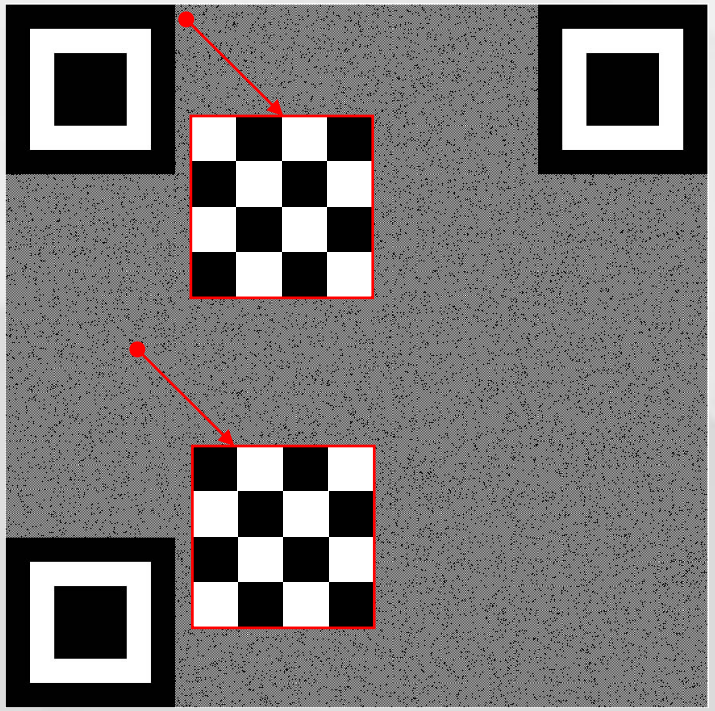
Photographs taken at other positions



Encryption Scheme of Moiré QR Code

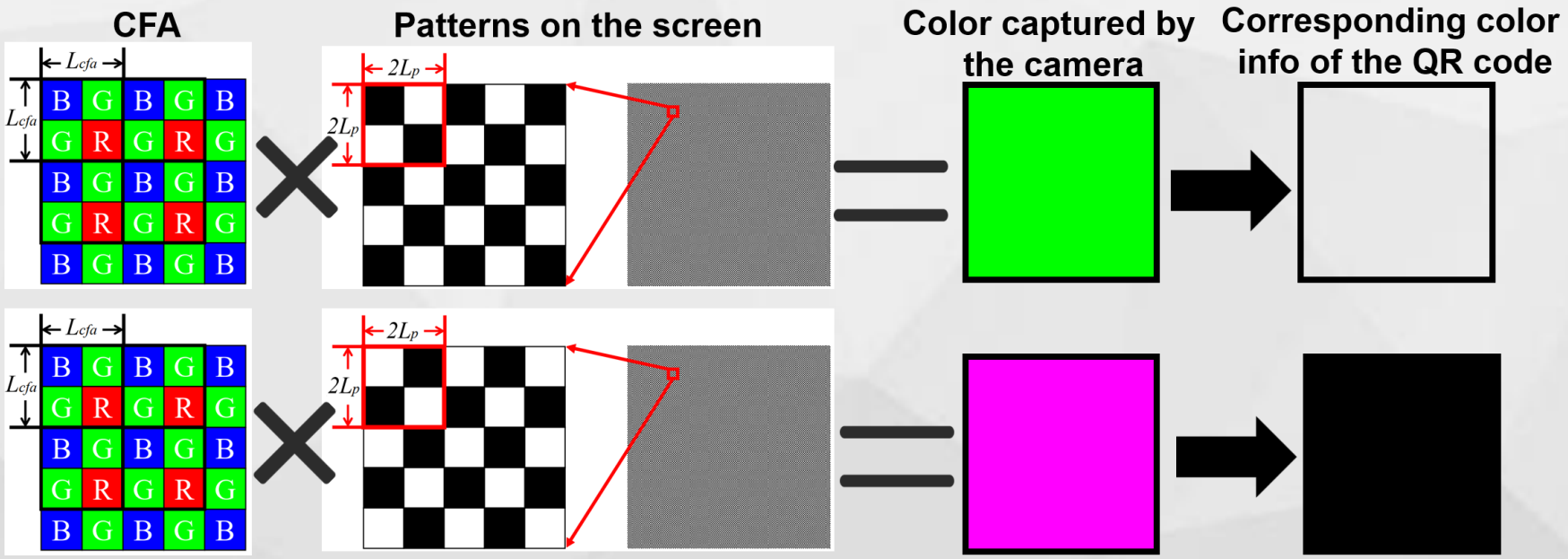


Original QR Code



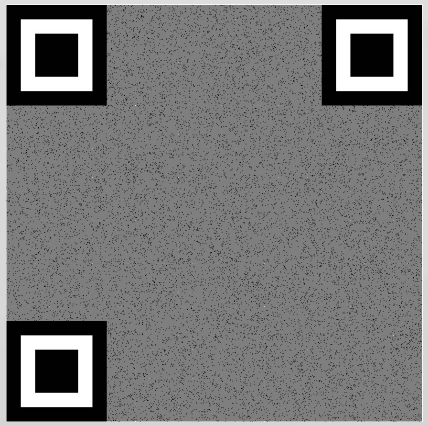
Encrypted QR Code

Encryption Scheme of Moiré QR Code

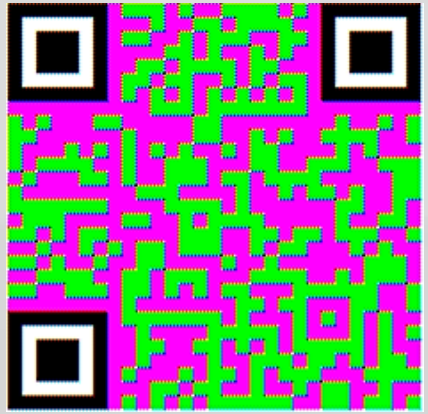


Standard QR Code

Encrypted QR Code

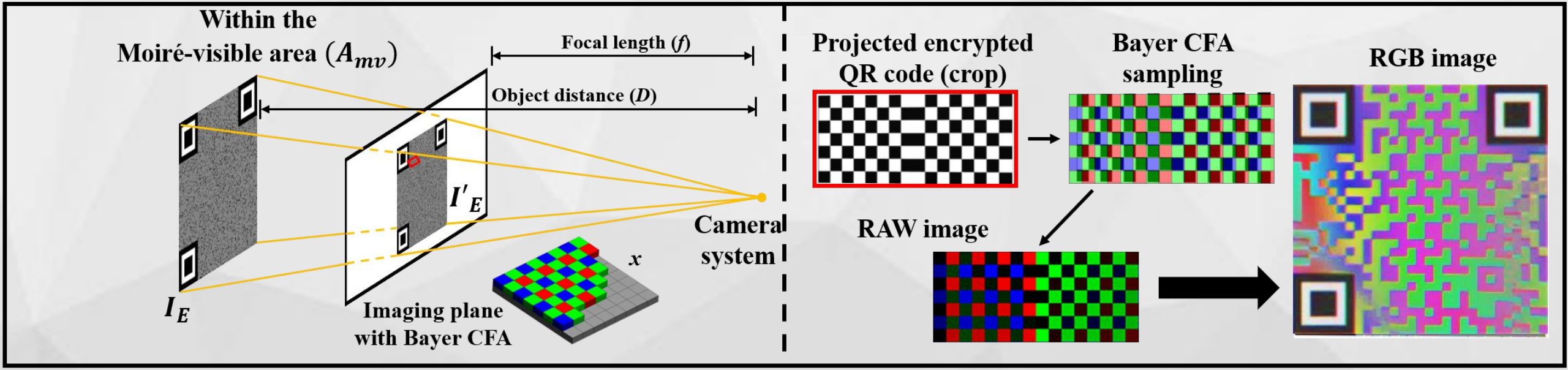


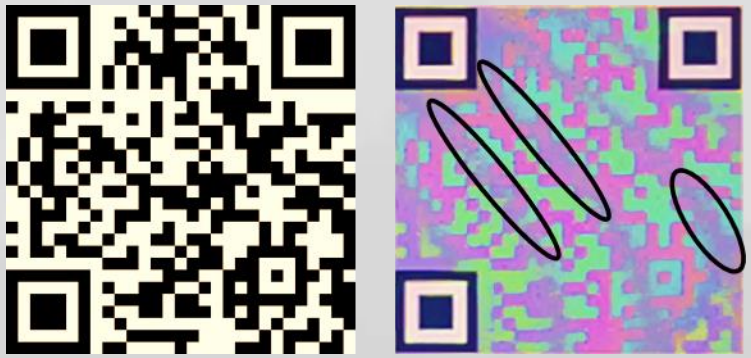
Moiré QR Code



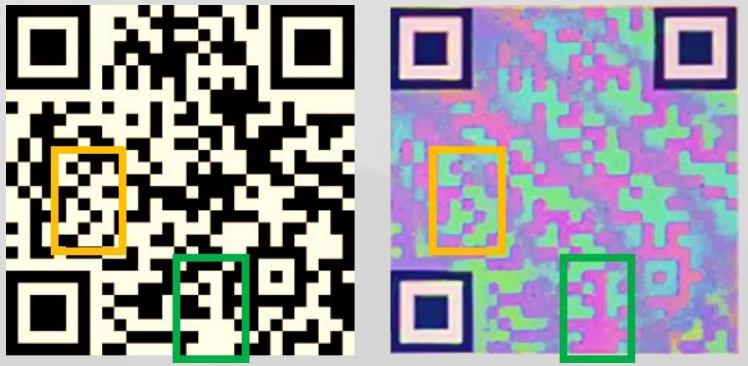
Perfect-match Pose

Blur and Color inversion



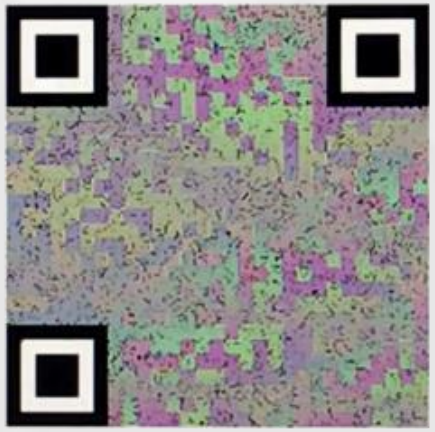


Blur phenomenon

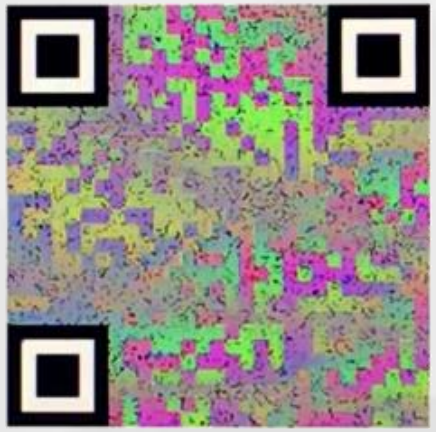


Color inversion phenomenon

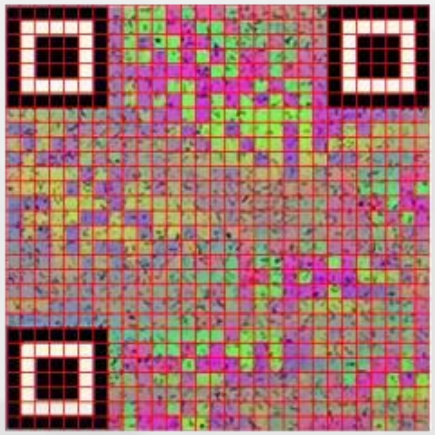
Traditional decryption process



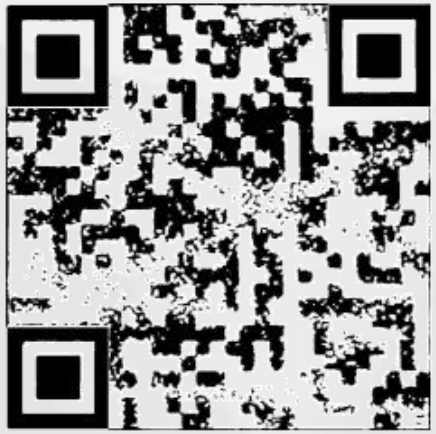
(a) *mQR* code taken by camera



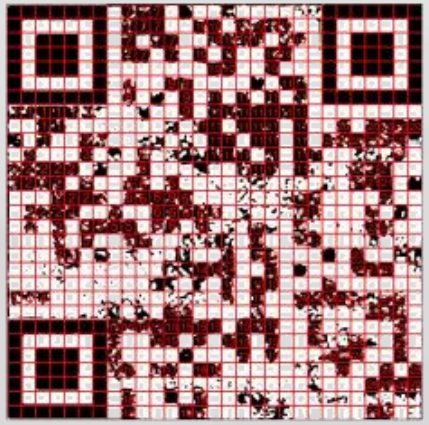
(b) Enhance saturation



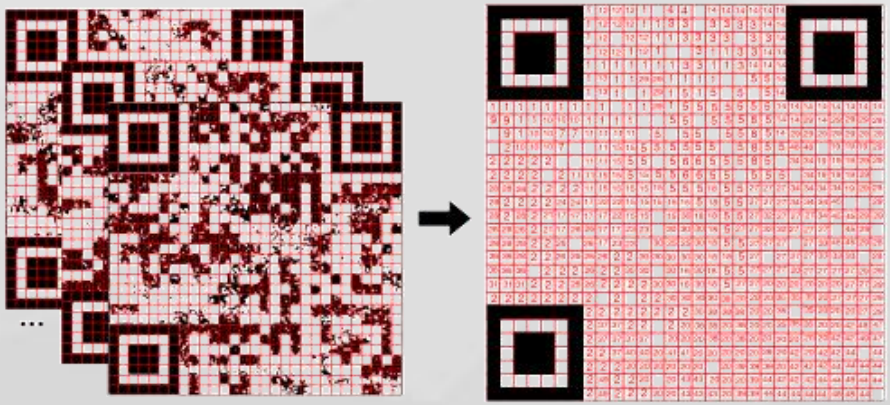
(c) Segment into blocks



(d) Convert into black and white



(e) Label adjacent blocks with the same color

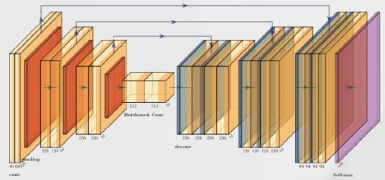


(f) Combine multiple frames

(g) Color blocks with black and white

Computationally complex & Slow (Latency 5.4s)!

New decryption process



Neural Network

Lower Decryption Latency

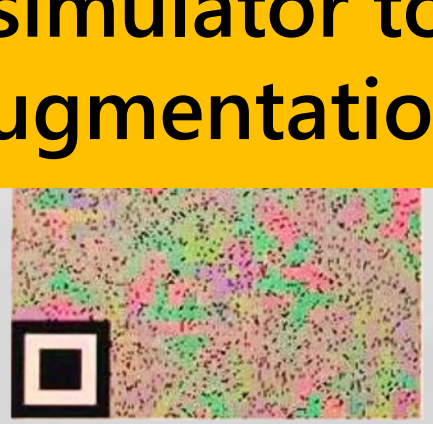
Higher Decryption Rate

Challenge: Data collection is high-cost

QR c

Our solution:

- ✓ Moiré simulator to solve position sensitivity
- ✓ Data augmentation to solve device diversity



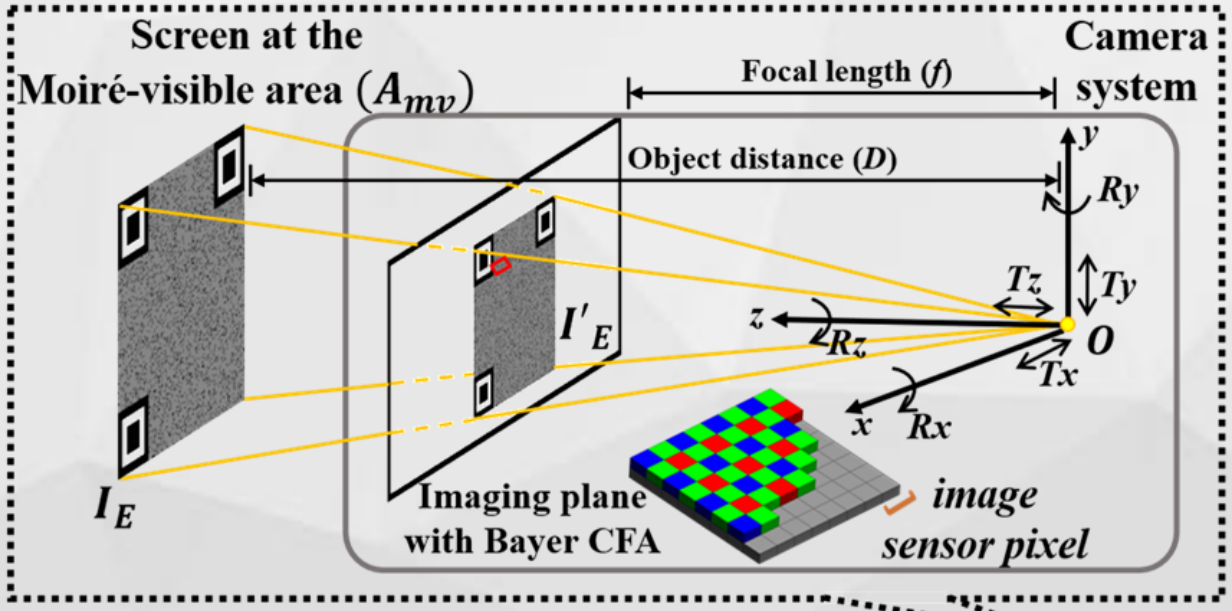
screen 1/position 1 screen 2/position 1

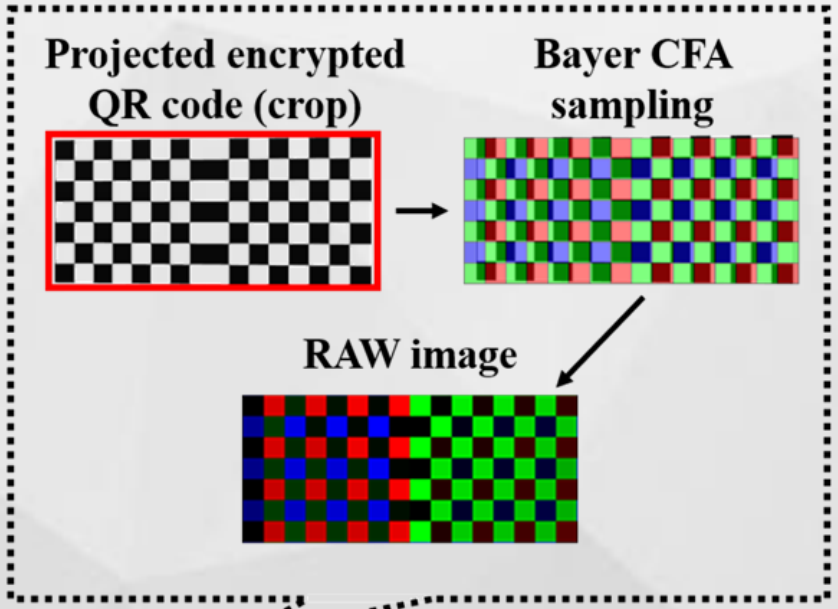
een

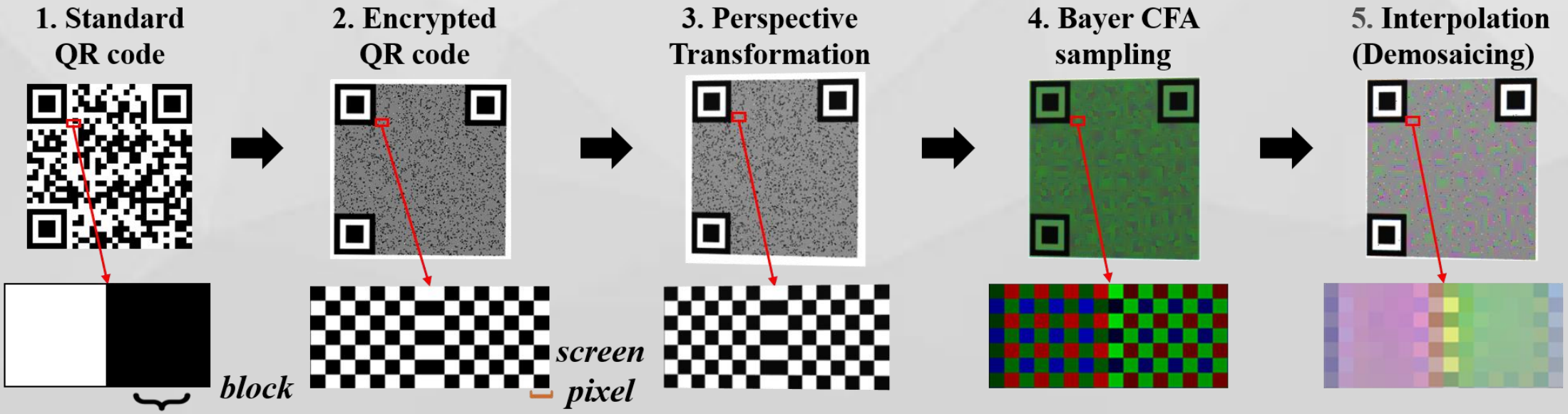
camera and screen

Device diversity: camera and screen

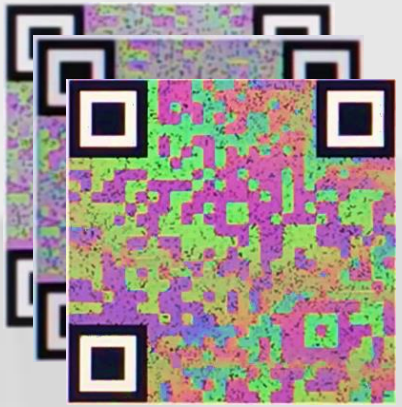
Moiré Simulator



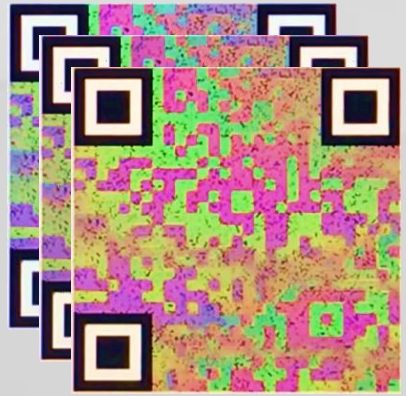




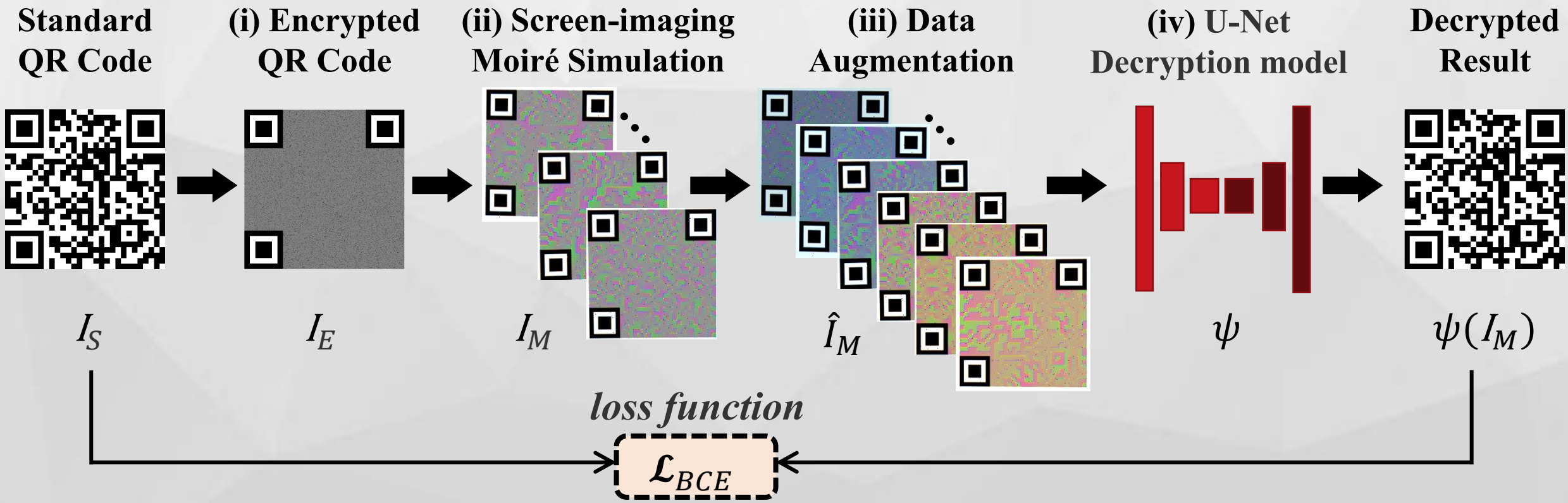
Data Augmentation



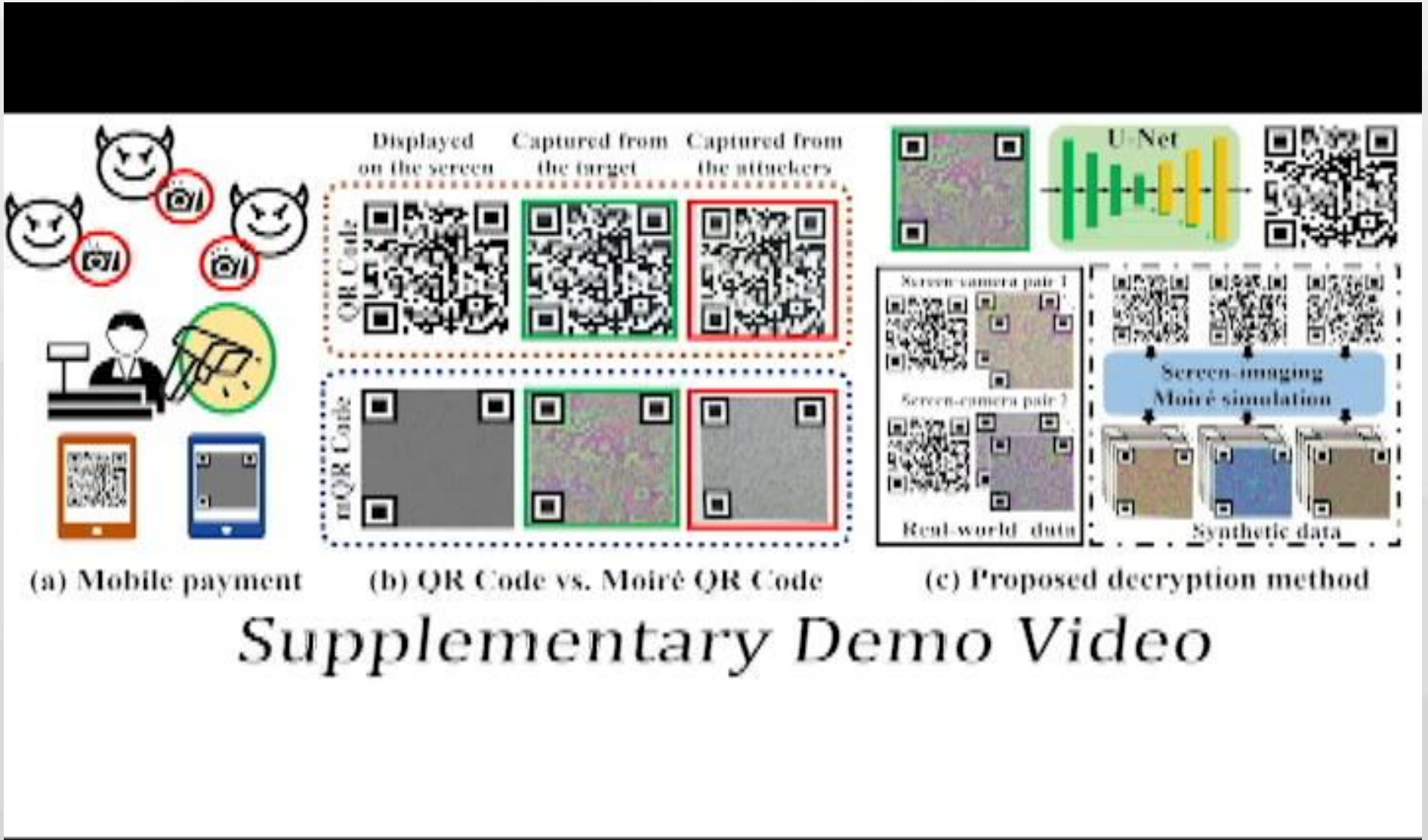
- Saturation
- Brightness and contrast
- Color temperature



The Training Process of Decryption Model



Demo

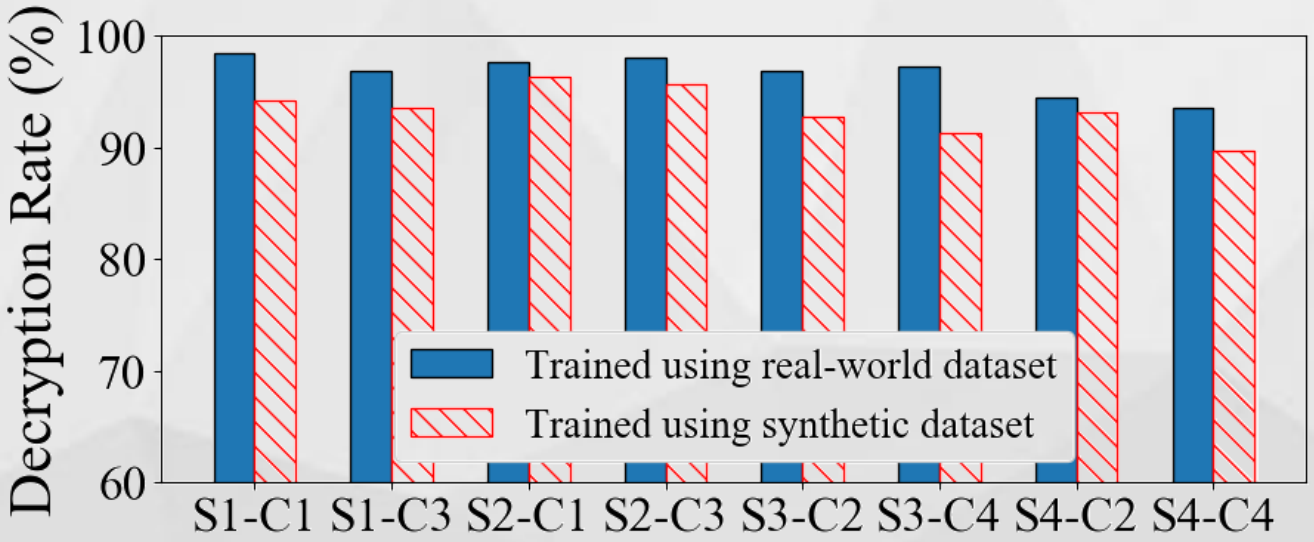

Displayed on the screen
Captured from the target
Captured from the attackers
QR Code
mQR Code
U-Net
Screen-camera pair 1
Screen-camera pair 2
Real-world data
Screen-imaging Moiré simulation
Synthetic data
(a) Mobile payment
(b) QR Code vs. Moiré QR Code
(c) Proposed decryption method
Supplementary Demo Video

Performance Evaluation

- Experiment Setup and Metrics:
  - ➢ We randomly generate 1000 original QR code images with version from 1 to 5.
  - ➢ For Synthetic Dataset, 800 original QR code images are used to simulate the Moiré QR code images.
  - ➢ For Real-world Dataset, 200 original QR code images are encrypted, displayed on the different digital screens and captured by different cameras.

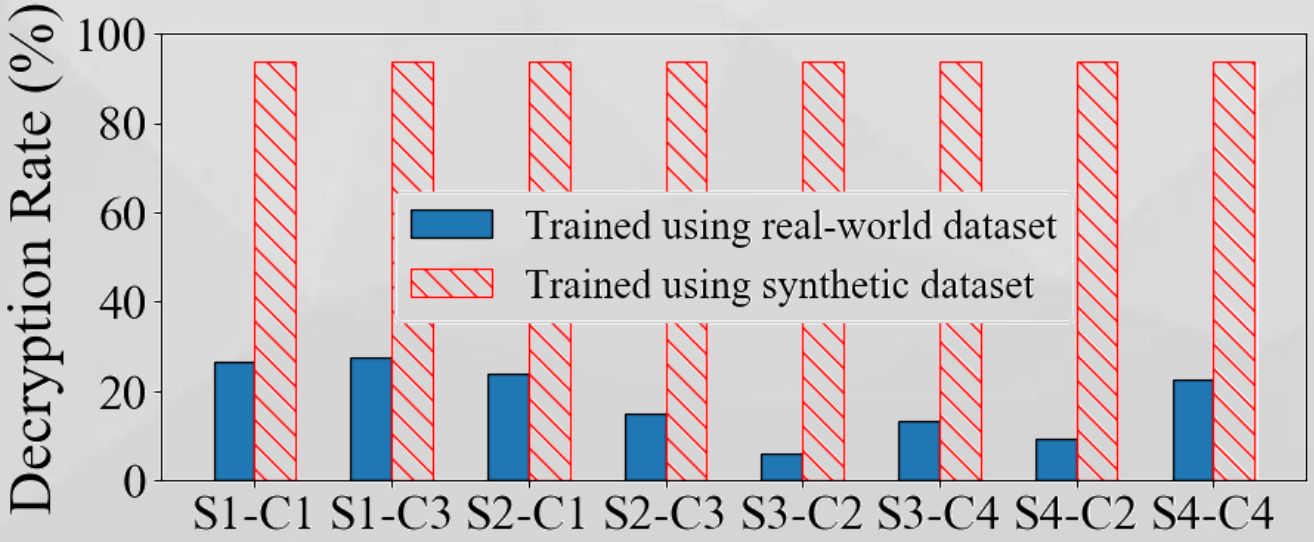
➢ Decryption Rate = $\frac{Number\ of\ QR\ codes\ successfully\ decrypted}{Number\ of\ all\ the\ test\ QR\ codes}$

Performance Evaluation - Real-world vs. Moiré Simulation



Test with the real-world dataset collected in the limited screen-camera relative poses.

$$synthetic \approx real - world$$

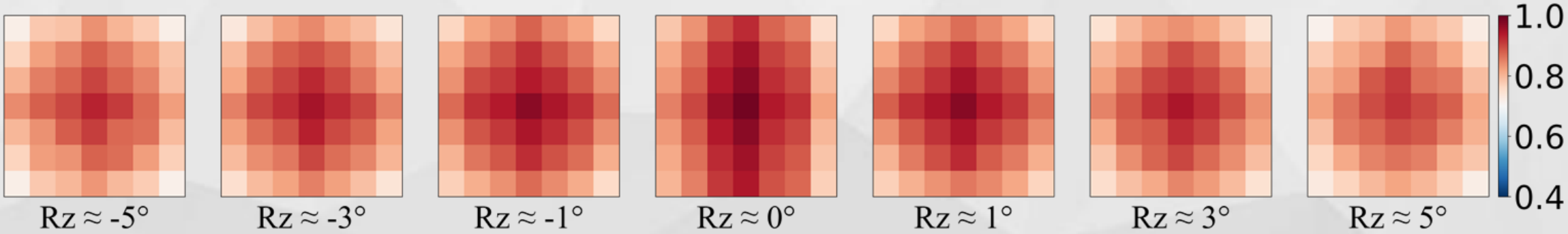


Test with the real-world dataset collected in the entire Moiré-visible area.

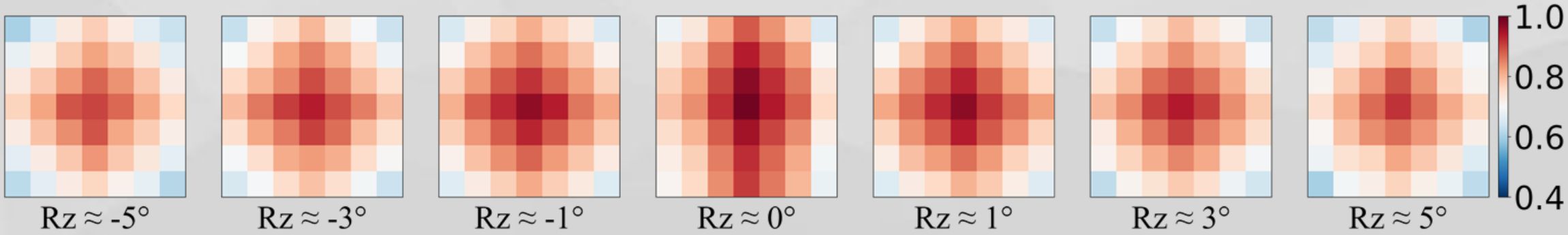
$$synthetic > real - world$$

Deep Learning Based vs. Traditional Multi-frame

The decryption rate of deep learning based decryption method for different angle offset.

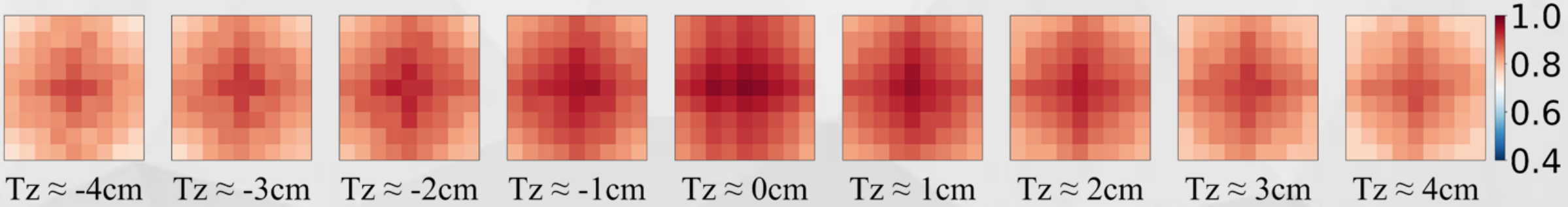


The decryption rate of traditional multi-frame decryption method for different angle offset.

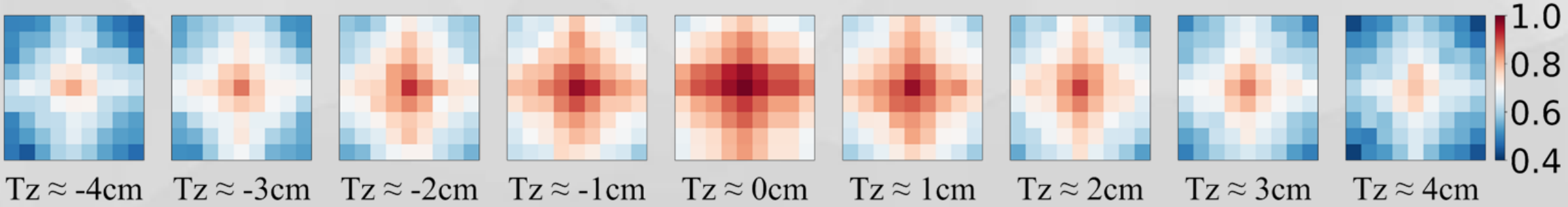


Deep Learning Based vs. Traditional Multi-frame

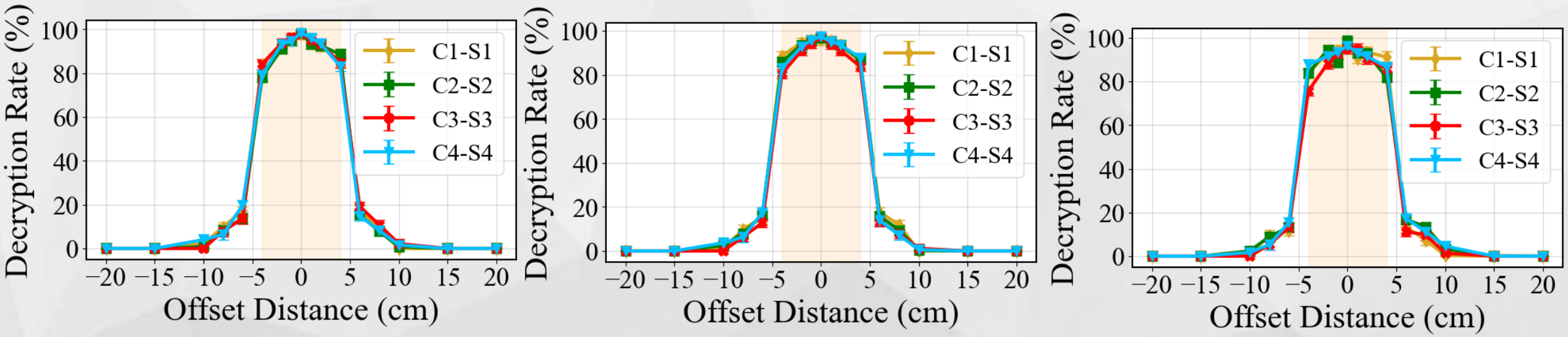
The decryption rate of deep learning based decryption method for different distance offset.



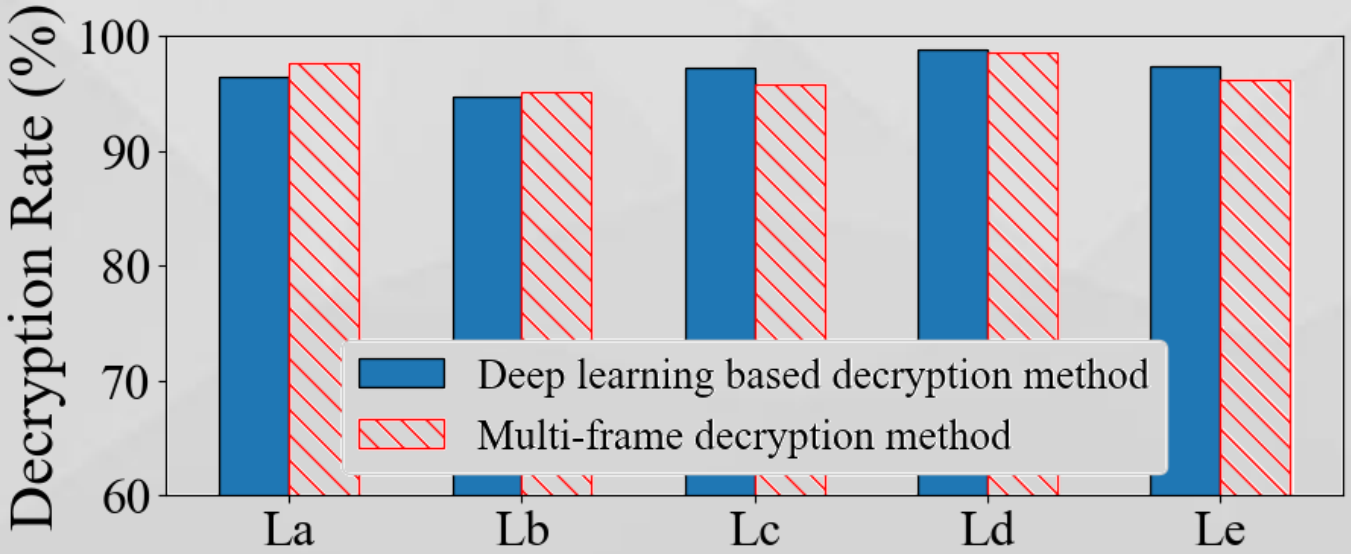
The decryption rate of traditional multi-frame decryption method for different distance offset.



Secure Scanning Range & Impact of Environment/Ambient



With high decryption rate in Moiré-visible Area and extremely low decryption rate out of the Moiré-visible Area, the Moiré QR code system is still secure.



La: Outdoor at 8AM;
Lb: Outdoor at 12AM;
Lc: Outdoor at 11PM;
Ld: Office;
Le: Indoor with all lights off.

Overall comparison

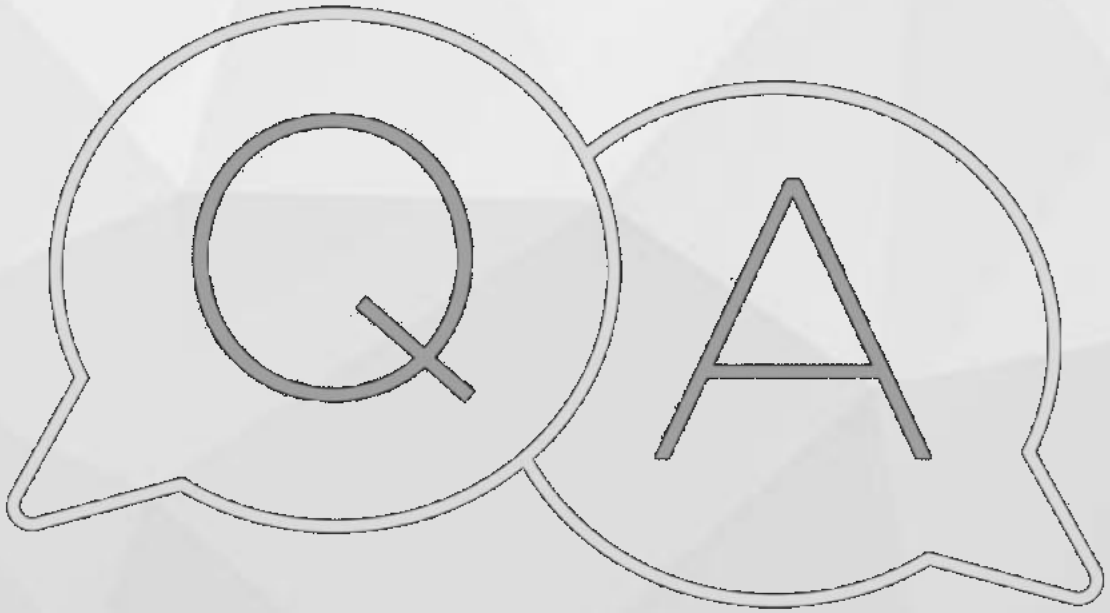
	Traditional Multi-frame	Deep Learning Based
Distance range	$[-2cm, 2cm]$	$[-4cm, 4cm]$
Angle range	$[-4°, 4°]$	$[-6°, 6°]$
Decryption rate	$98.6\%(11.3\ frames)$	$\mathbf{98.8\%}(2\ frames)$
Decryption latency	$5.4 \pm 0.07s$	$\mathbf{0.02} \pm 0.006s$
RAM	$27.4MB$	$224.2MB$

Conclusion

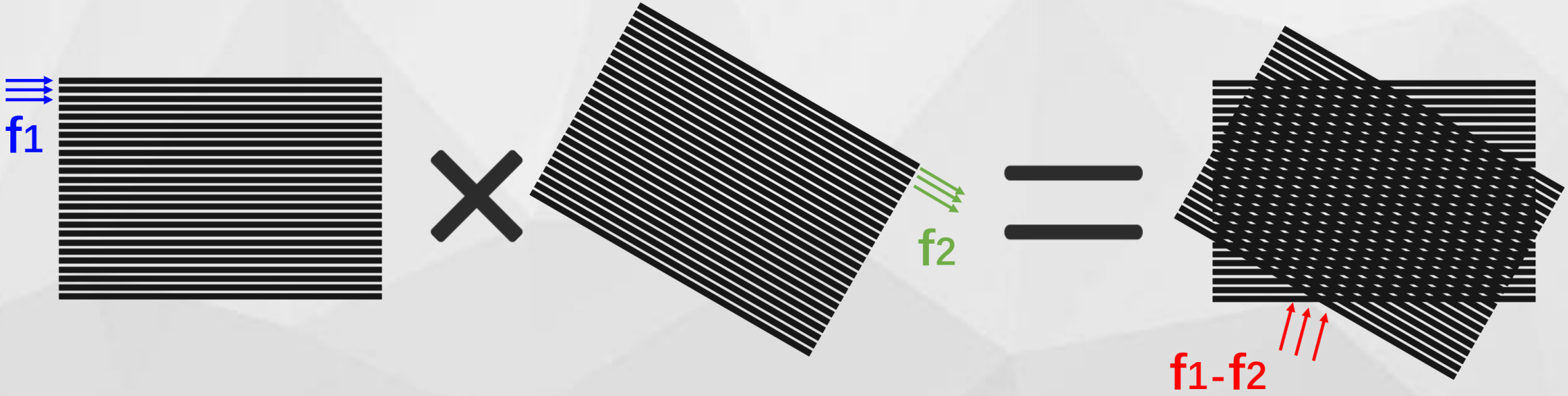
- We propose a deep learning based Moiré QR code decryption method which can reduce the average decryption latency.
- We propose a screen-imaging Moiré simulation methodology that approximates the “physical transmission”, and synthesize Moiré QR code images to improve the robustness of the training dataset.
- We conduct extensive experiments to verify the effectiveness of the screen-imaging Moiré simulation.

Thanks

For Watching!


Q
A

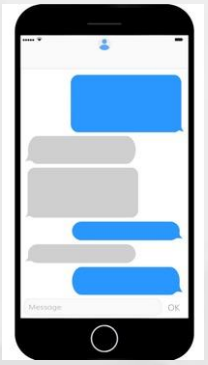
Encryption Principle



$$m = m_1 \times m_2$$
$$= (a_1 + b_1 \cos 2\pi f_1 t) \times (a_2 + b_2 \cos 2\pi f_2 t)$$
$$= a_1 a_2 + a_2 b_1 \cos 2\pi f_1 t + a_1 b_2 \cos 2\pi f_2 t +$$
$$b_1 b_2 \cos 2\pi (f_1 + f_2) t + b_1 b_2 \cos 2\pi (f_1 - f_2) t$$

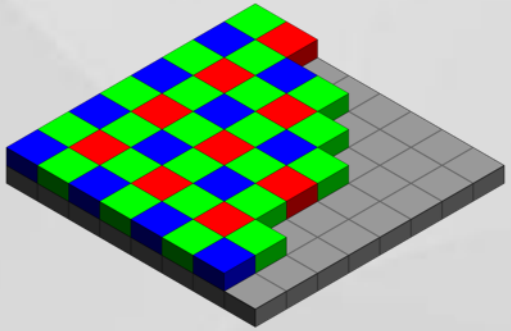
Encryption Principle

Camera



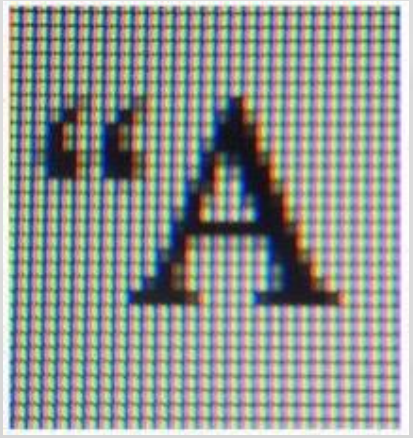
Display

Low-frequency Colorful Noise Patterns



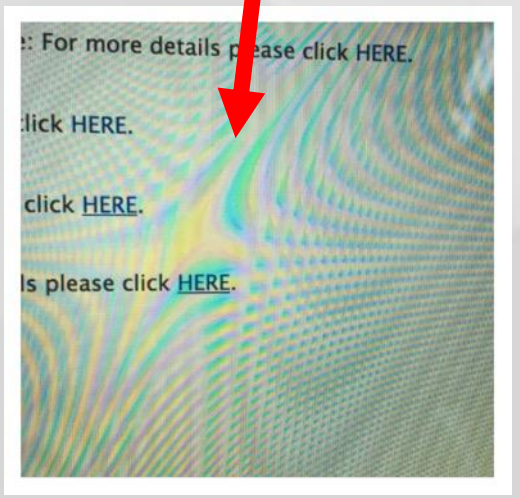
Color Filter Array

×

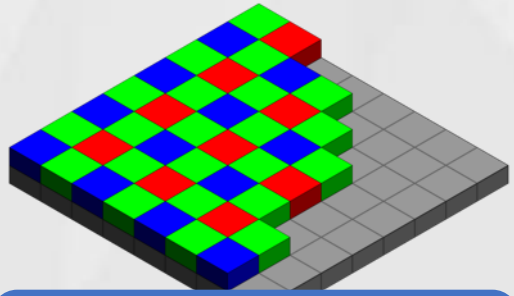


Pixel Array

=



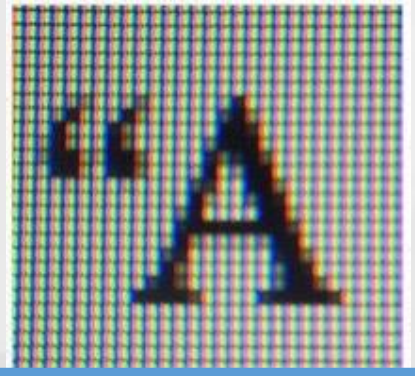
Encryption Principle



Known

$m_1(x, y)$

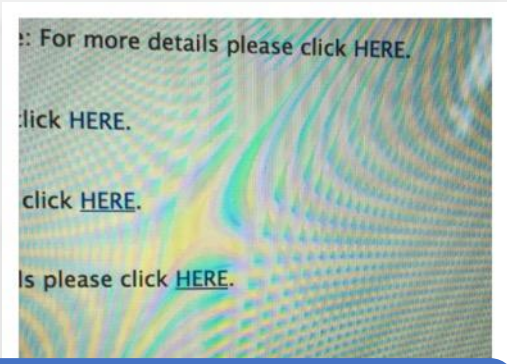
×



Computed

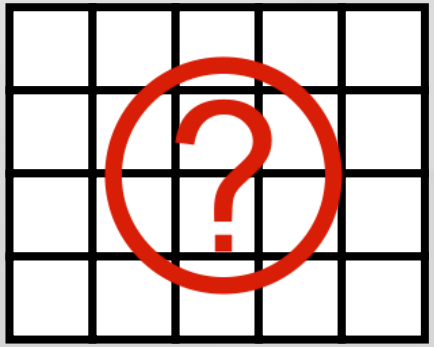
$m_2(x, y)$

=



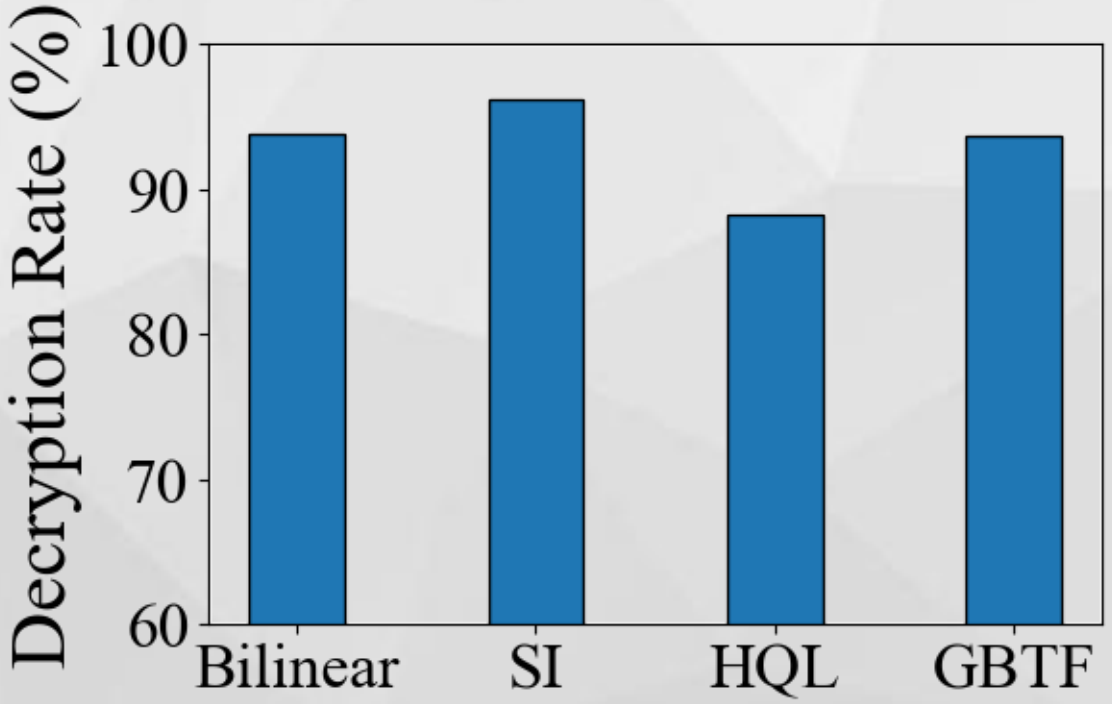
Known

$m_3(x, y) = m_1(x, y) \times m_2(x, y)$

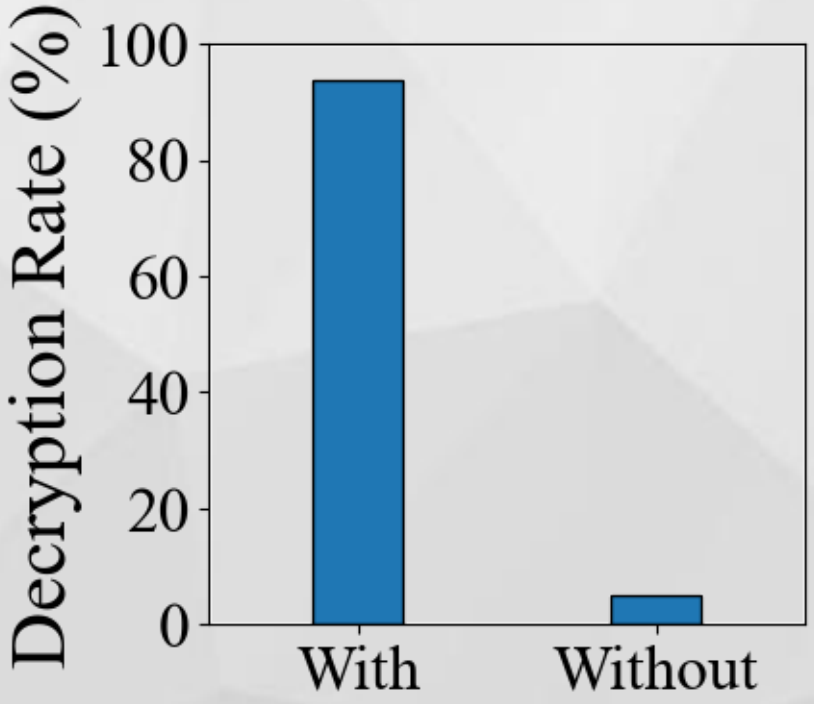


mQR Code

Evaluation: Interpolation algorithm & Data Augmentation



All interpolation algorithms provide a satisfactory decryption performance.



The data augmentation module is indeed an essential part of the simulator.