ABC: Enabling Smartphone Authentication with Built-in Camera

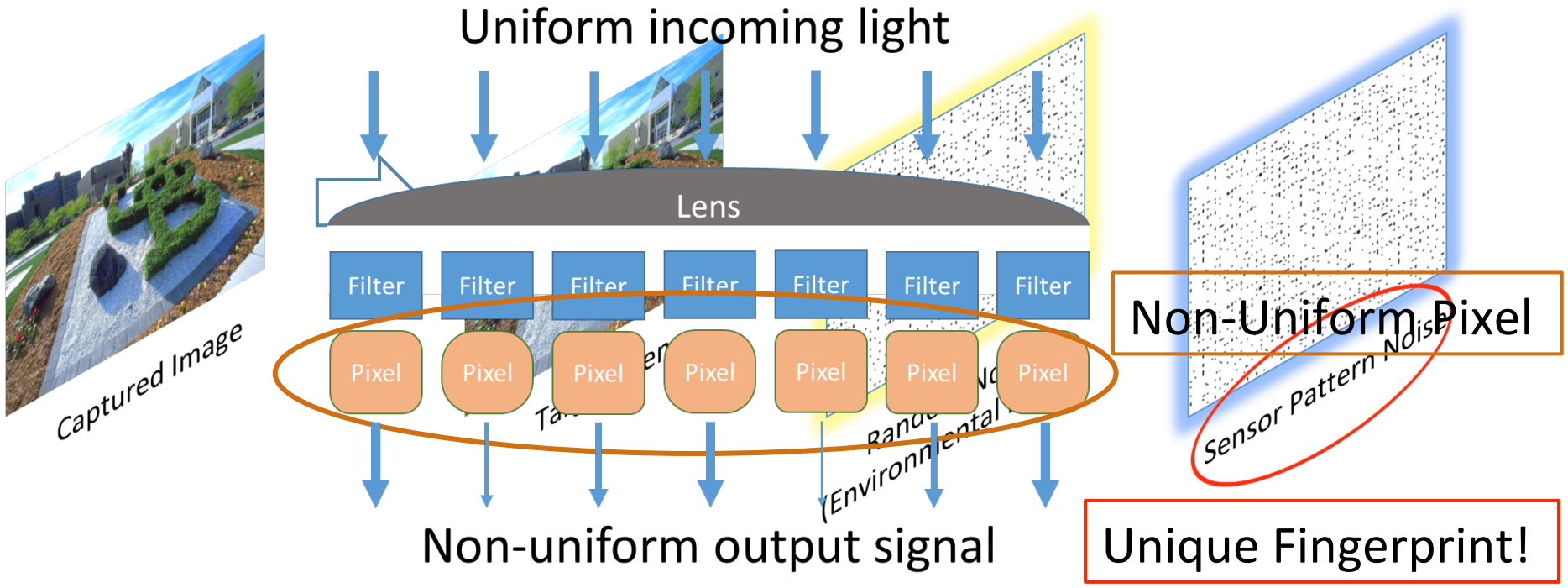
Zhongjie Ba[*] , *Sixu Piao*[*] , *Xinwen Fu*[†] , *Dimitrios Koutsonikolas*[*] , *Aziz Mohaisen*[†] and *Kui Ren*[*]

[*] University at Buffalo
The State University of New York

[†] University of Central Florida

Camera Identification: Hardware Distortion

- Manufacturing imperfection leads to pattern noise: Photo Response Non-Uniformity (PRNU)[1]



[1] LUKAS, J., FRIDRICH, J., AND GOLJAN, M. Digital camera identifi- cation from sensor pattern noise. IEEE Transactions on Information Forensics and Security 1, 2 (2006), 205–214.

Camera Identification: Fingerprint Matching

- Given an image, determine if it is captured by a camera of interest

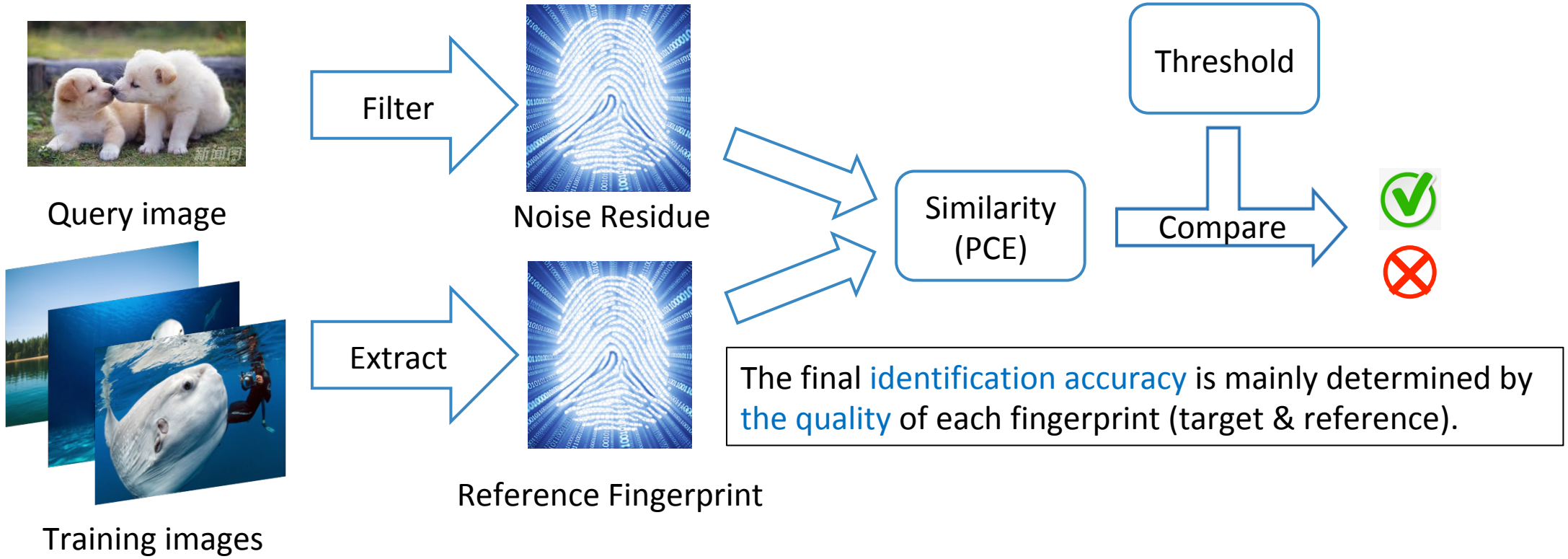


Image source: https://www.packtpub.com/networking-and-servers/mastering-python-forensics;

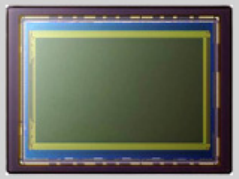
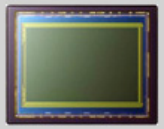
From Camera Identification to Smartphone Identification

- Smartphone cameras have displaced the conventional digital camera

- Smartphones are widely used in security sensitive tasks

Image source: https://techdigg.com/2017/05/12/apple-wants-you-to-be-a-professional-iphone-7-photographer/; https://www.nextpowerup.com/news/28115/google-brings-android-pay-to-uk/

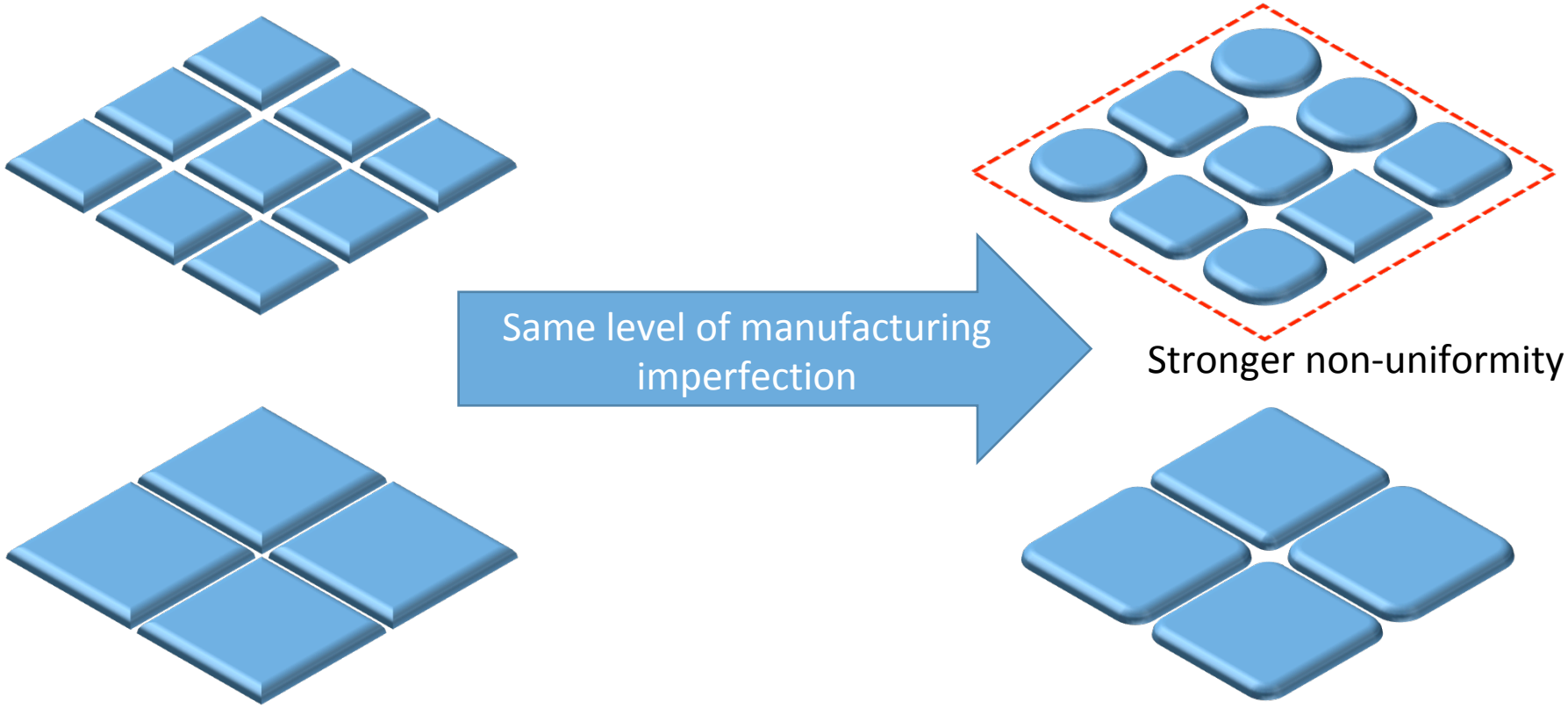
Smartphone Camera VS Digital Camera

Sensor Name	Medium Format	Full Frame	APS-H	APS-C	4/3	1"	1/1.63"	1/2.3"	1/3.2"
Sensor Size	53.7 x 40.2mm	36 x 23.9mm	27.9x18.6mm	23.6x15.8mm	17.3x13mm	13.2x8.8mm	8.38x5.59mm	6.16x4.62mm	4.54x3.42mm
Sensor Area	21.59 cm²	8.6 cm²	5.19 cm²	3.73 cm²	2.25 cm²	1.16 cm²	0.47 cm²	0.28 cm²	0.15 cm²
Crop Factor	0.64	1.0	1.29	1.52	2.0	2.7	4.3	5.62	7.61
Image									
Example									

https://lensvid.com/technique/why-depth-of-field-is-not-effected-by-sensor-size-a-demonstration/

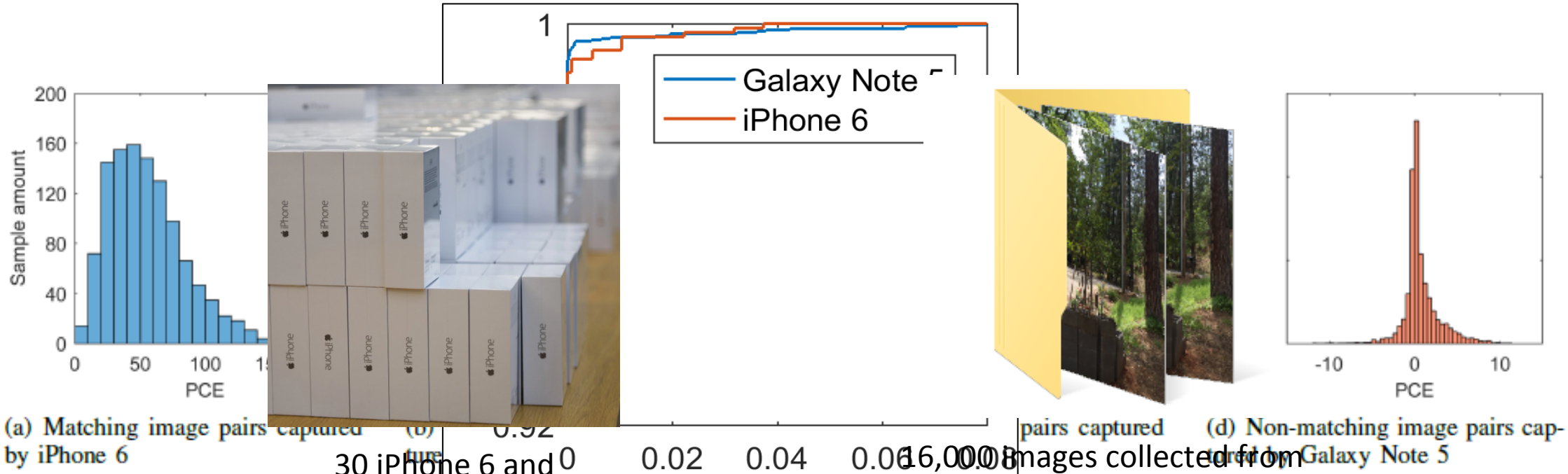
Smartphone Camera: Stronger Non-Uniformity

- The reduction in dimension amplifies the pixels' non-uniformity



Smartphone Camera: Higher Identification Accuracy

- One image alone can uniquely identify a smartphone camera

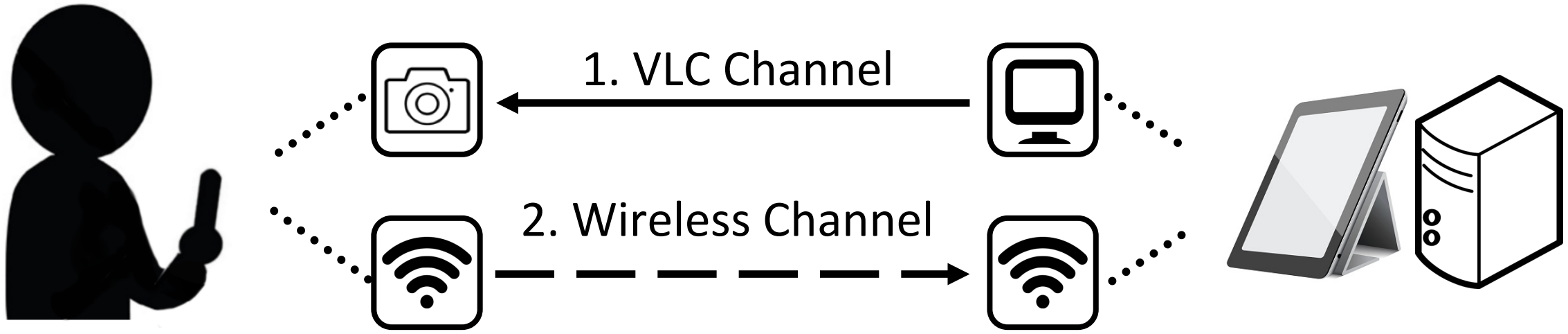


30 iPhone 6 and 10 Galaxy Note 5

16,000 images collected from **Amazon Mechanical Turk**

Smartphone Authentication Scenario

- The user proves her identity to the verifier using her smartphone as a security token
- The verifier authenticates the user's smartphone by checking the fingerprint of its built-in camera



A Strawman Solution

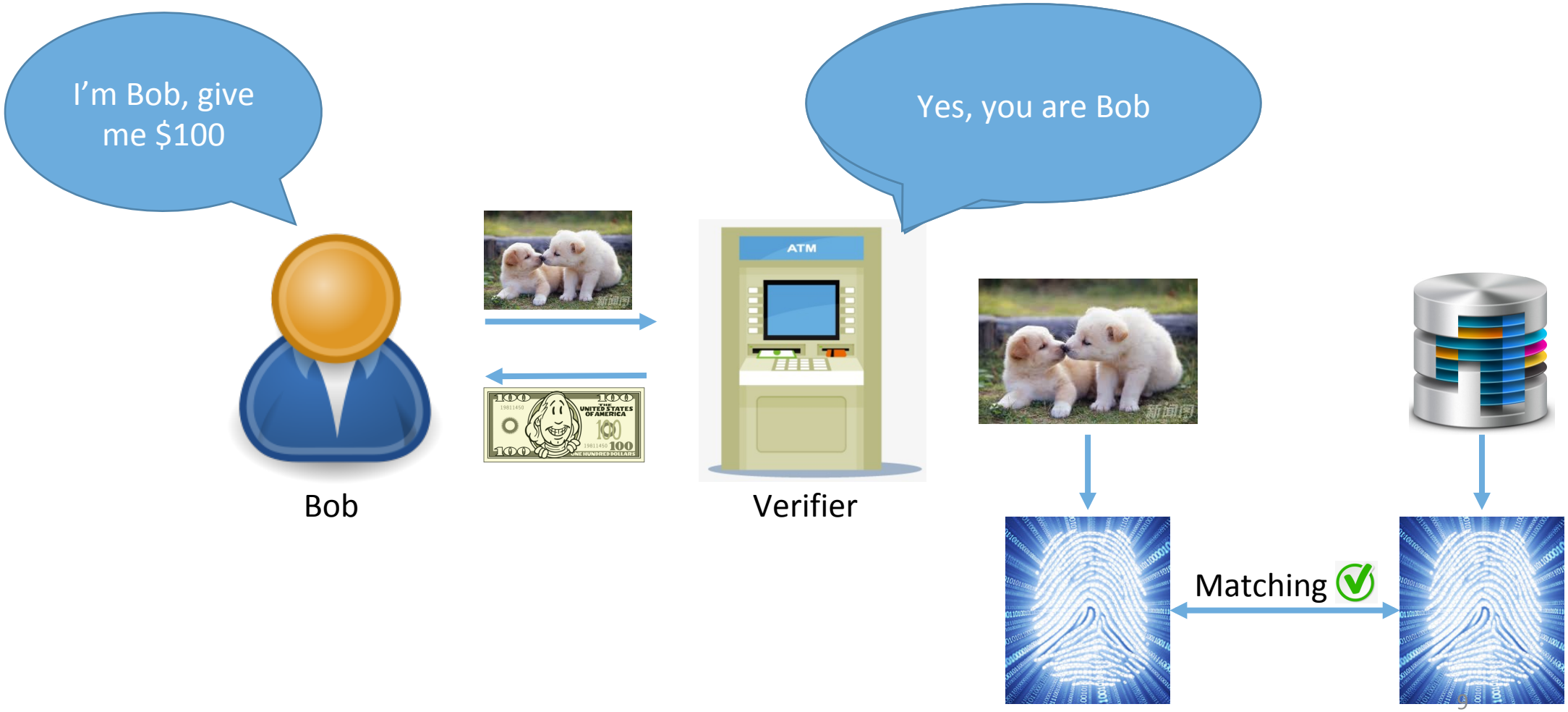
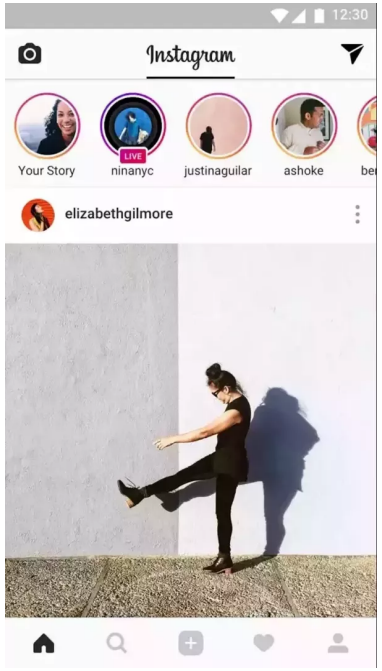


Image source: http://588ku.com/sucai/4051615.html; https://cn.vectorhq.com/istock/cartoon-ben-franklin-100-dollar-bill-116281;

Security Risk 1: Fingerprint Leakage

- Images captured by smartphone cameras, in most cases, are available to the public

Facebook

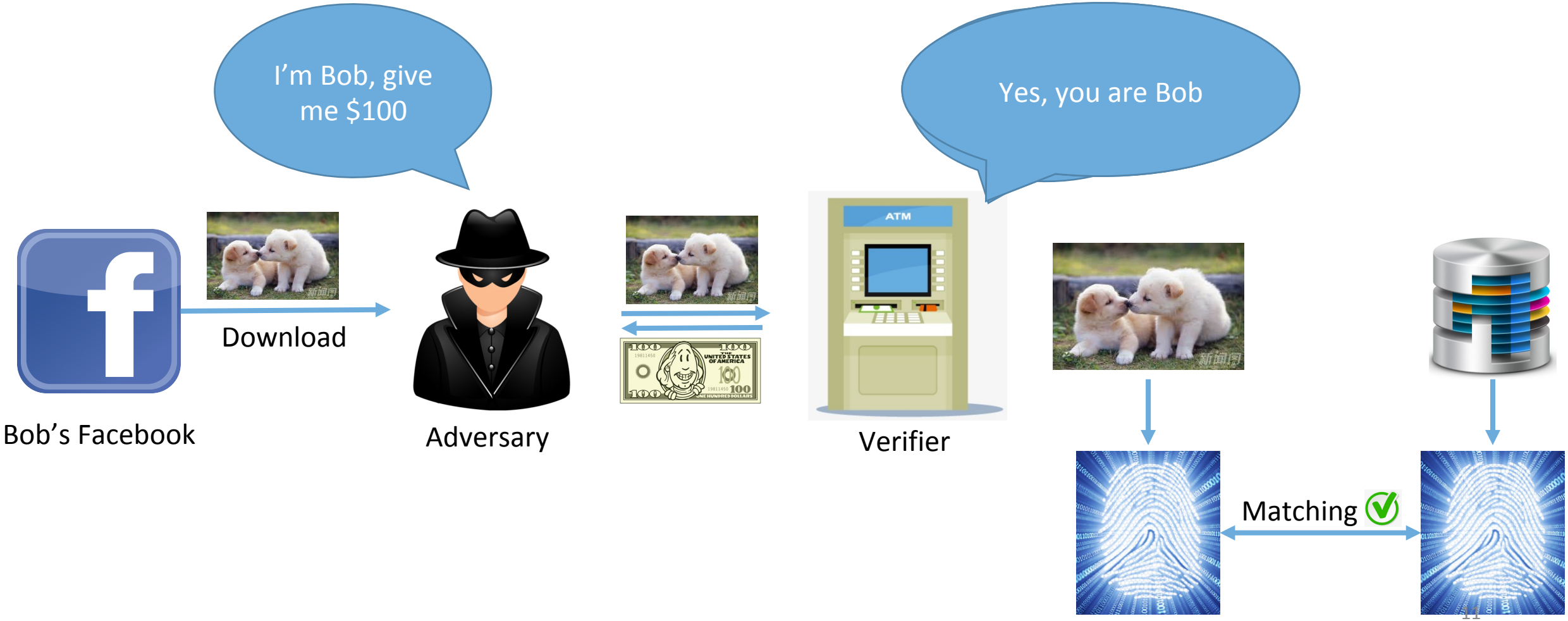


Instagram

Wechat

Image source: http://www.148apps.com/app/284882215/; http://dzapk.com/applications/instagram-black-mod-v11-0-0-3-20.html; http://www.woshipm.com/operate/215491.html

Fingerprint Leakage: The Replay Attack



Solution: Randomized QR Code

- Liveness detection:
  - Challenge the user to capture a freshly generated QR code

Accurate

Efficient

Easy to randomize

Easy to align

Image submitted to the authentication system should match the challenge

Image source: http://aleksandarpetkovic.com/category/ambiental-media/

Security Risk 2: Fingerprint Forgery

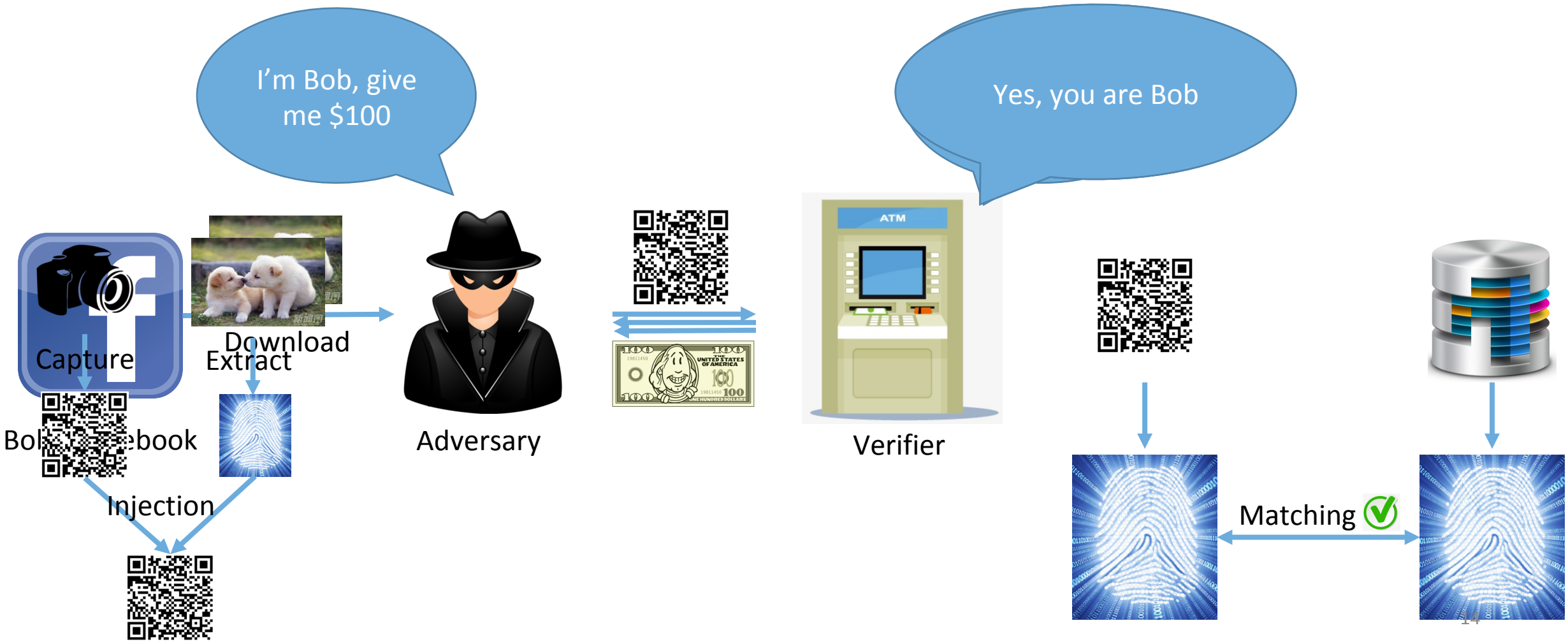
- An adversary can manipulate an image's fingerprint and fabricate forged images

Fingerprint Injection

Fingerprint Removal

Image source: http://www.jiguo.com/article/article/51934.html; http://www.dizzle.com/dizzle-launches-new-white-glove-concierge-service/

Fingerprint Forgery: The Injection Attack



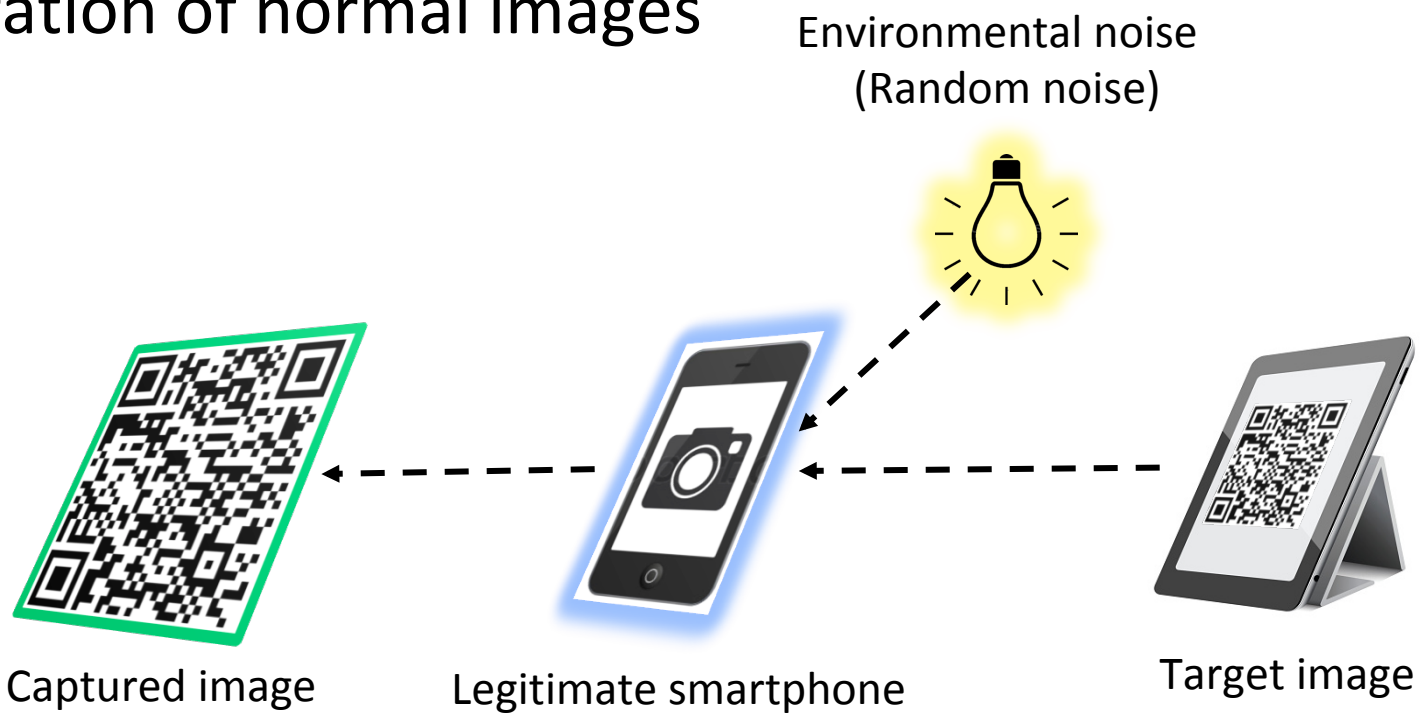
Injection Detection

- Detect forged images that carry injected fingerprints

Image source: http://www.entornointeligente.com/articulo/185619/VENEZUELA-Amenazas-muy-graves-incluso-a-su-vida-Escarra-denuncia-acoso-contra-sus-2-hijas-en-EEUU

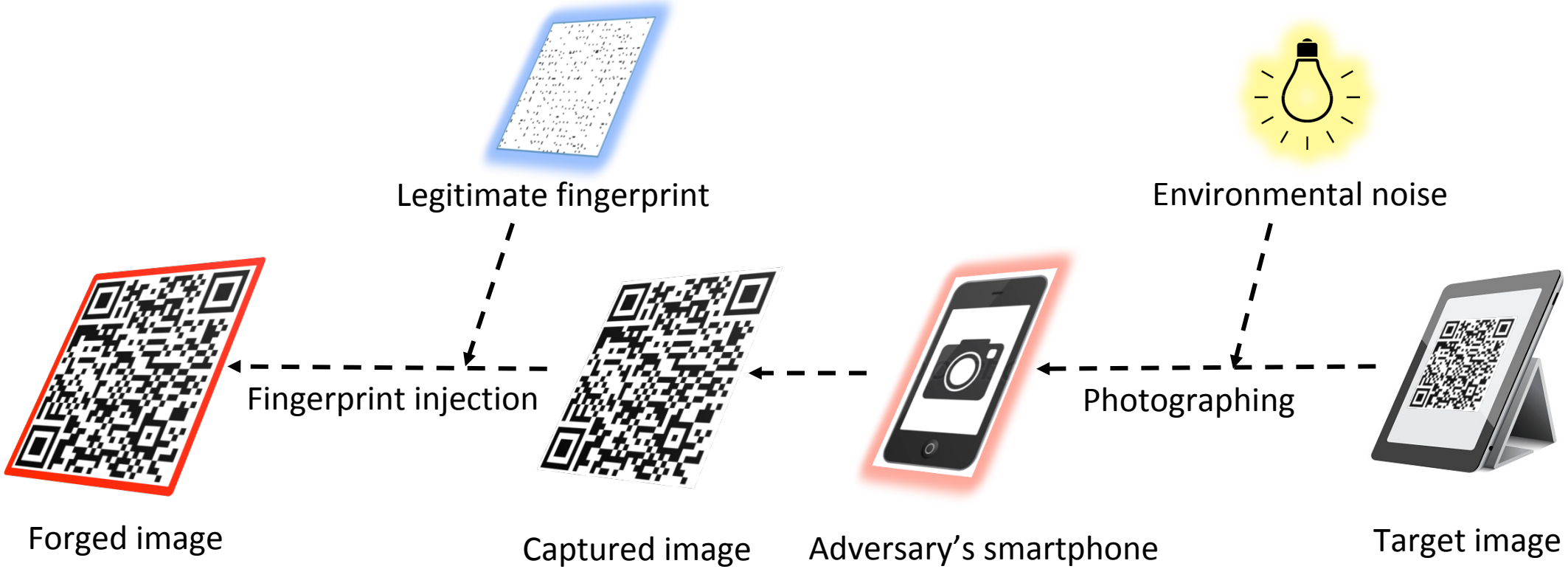
Normal Image VS Forged Image

- The generation of normal images



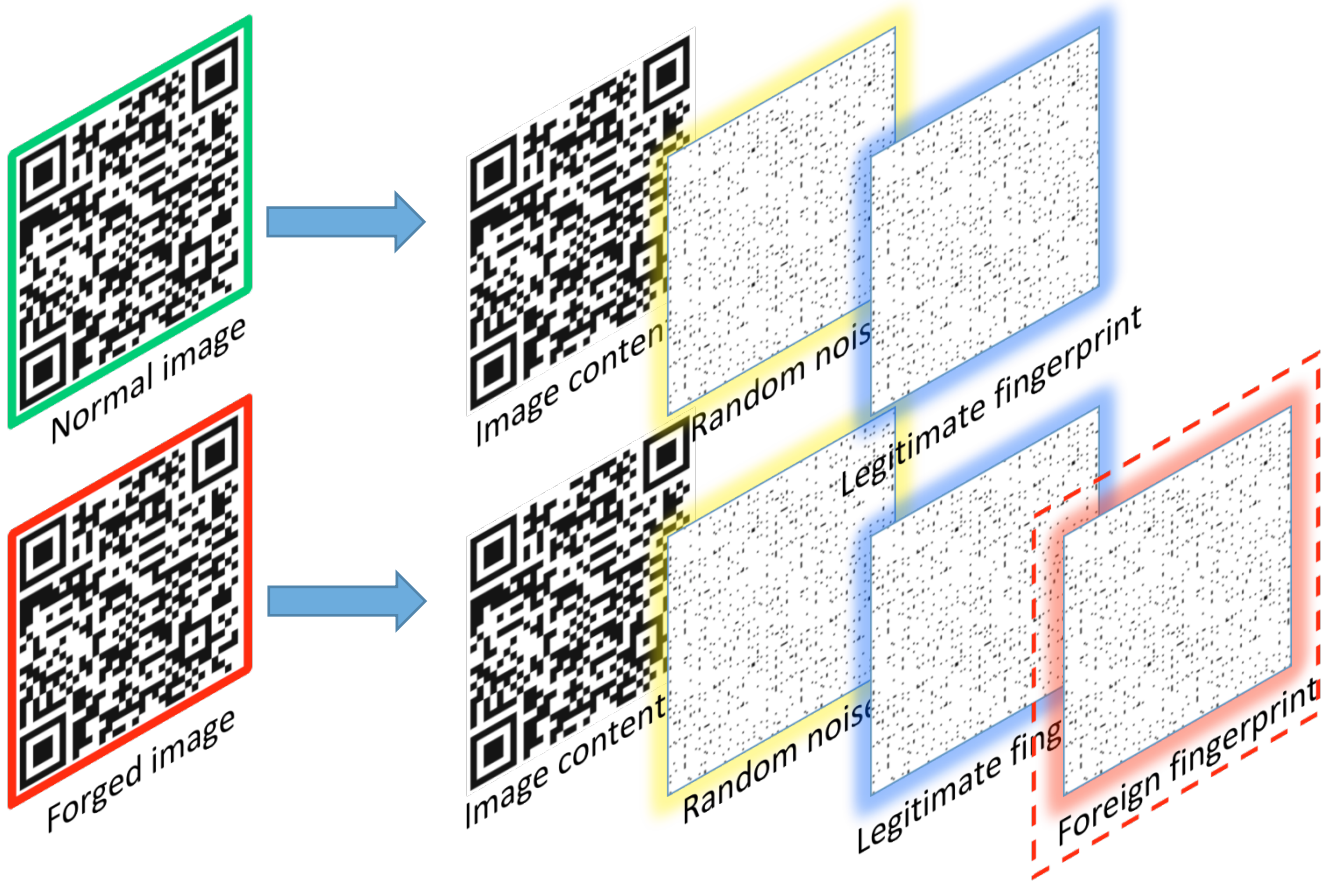
Normal Image VS Forged Image

- The generation of forged images



Normal Image VS Forged Image

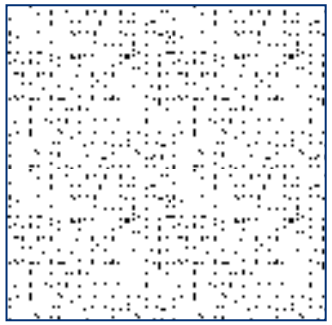
- Forged images carry the foreign fingerprint of the adversary's smartphone camera



Solution: Correlation Test

- Revised challenge response process:
  - Challenge the user to capture and upload two freshly generated QR codes.

Solution: Correlation Test

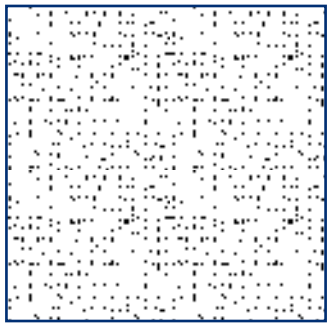


Reference Fingerprint

Correlation 1 (PCE1)

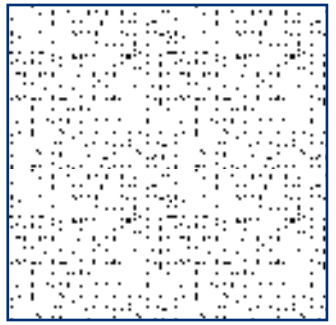
Captured image 1

Extract



Noise residue 1

Correlation 2 (PCE2)

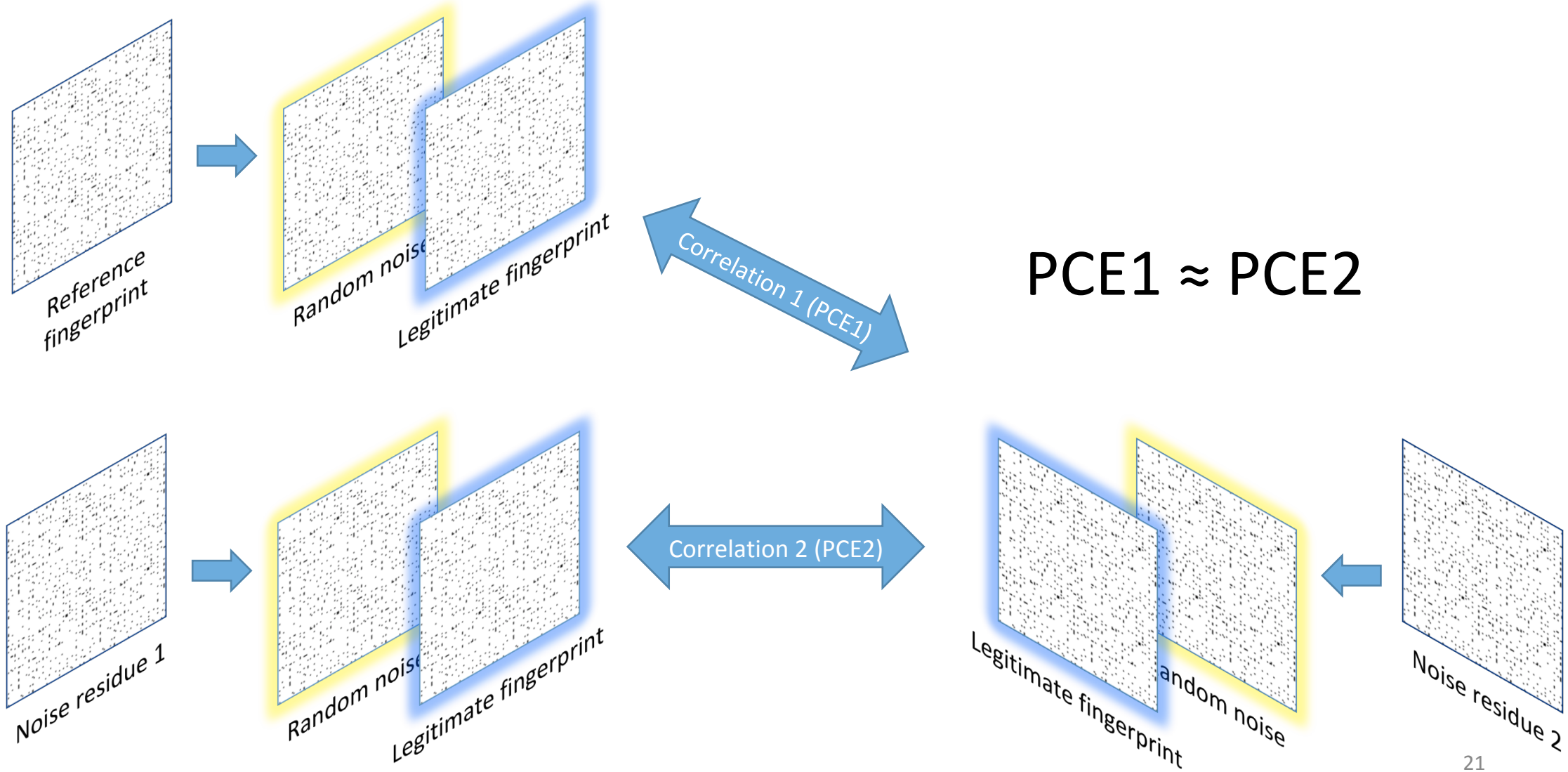


Noise residue 2

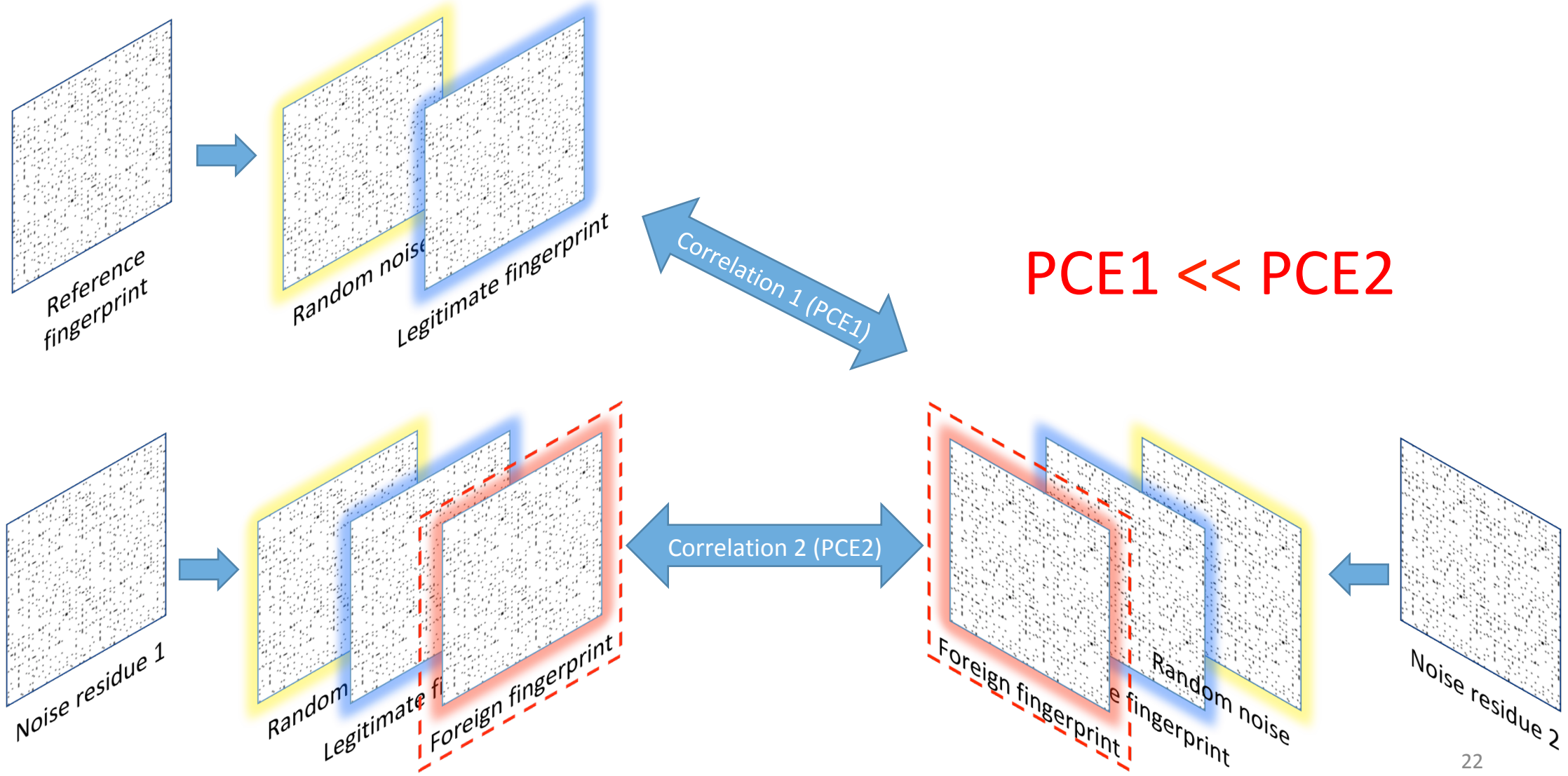
Extract

Captured image 2

Injection Detection: Normal Image Pair

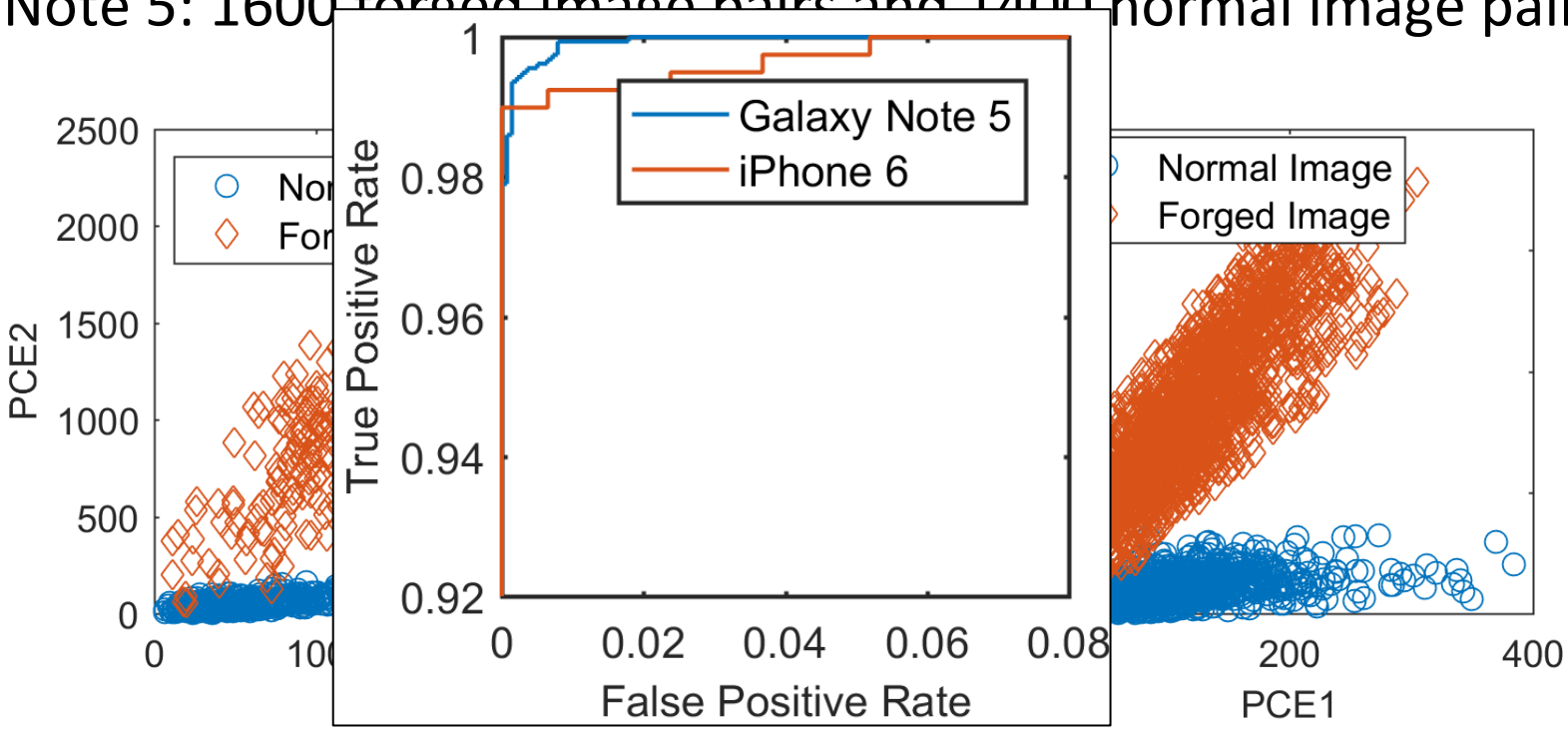


Injection Detection: Forged Image Pair



Effectiveness of Injection Detection

- 16,000 images from **Amazon Mechanical Turk**
  - iPhone 6: 400 forged image pairs and 450 normal image pairs
  - Galaxy Note 5: 1600 forged image pairs and 1400 normal image pairs



iPhone 6 Galaxy Note 5

Authentication Work Flow

What if the adversary removes his camera fingerprint?

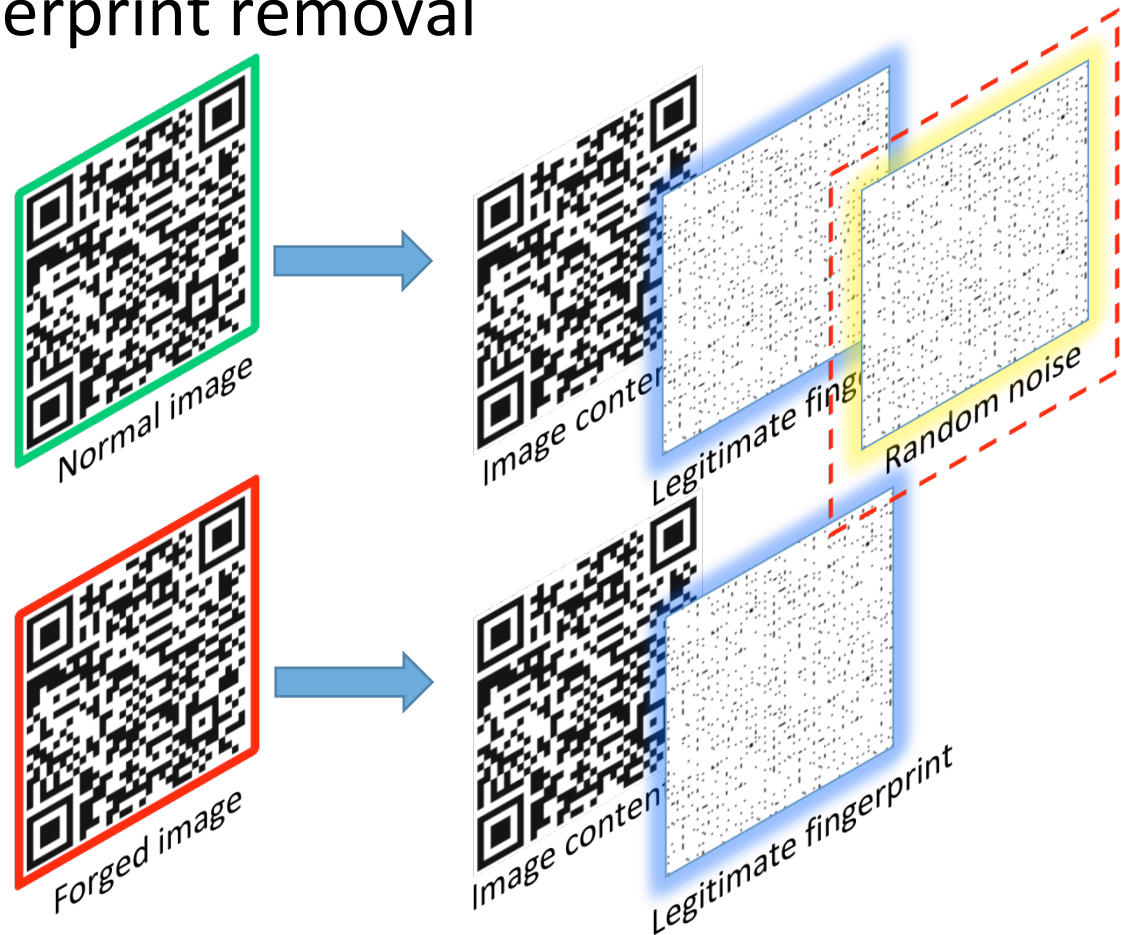
Removal Detection

- Detect forged images that have been sanitized (fingerprint removal)

Image source https://swimmingupstreamlife.com/2016/07/03/fingerprints/

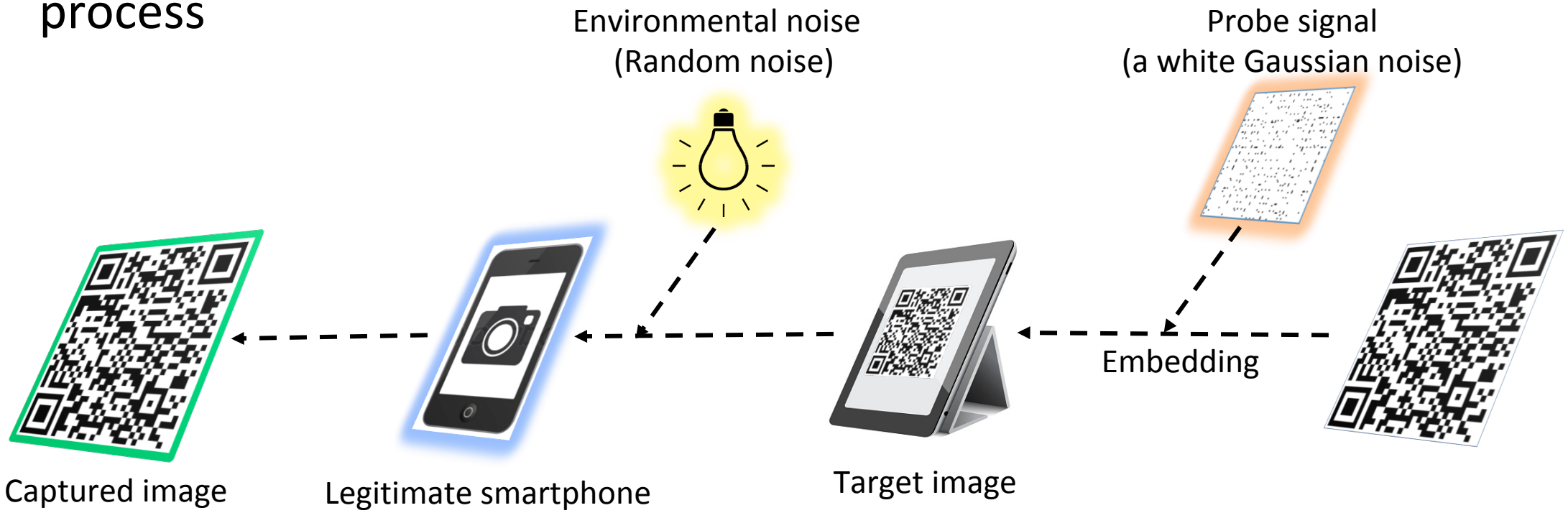
Normal Image VS Forged Image

- All white Gaussian noise components will be removed in the process of fingerprint removal



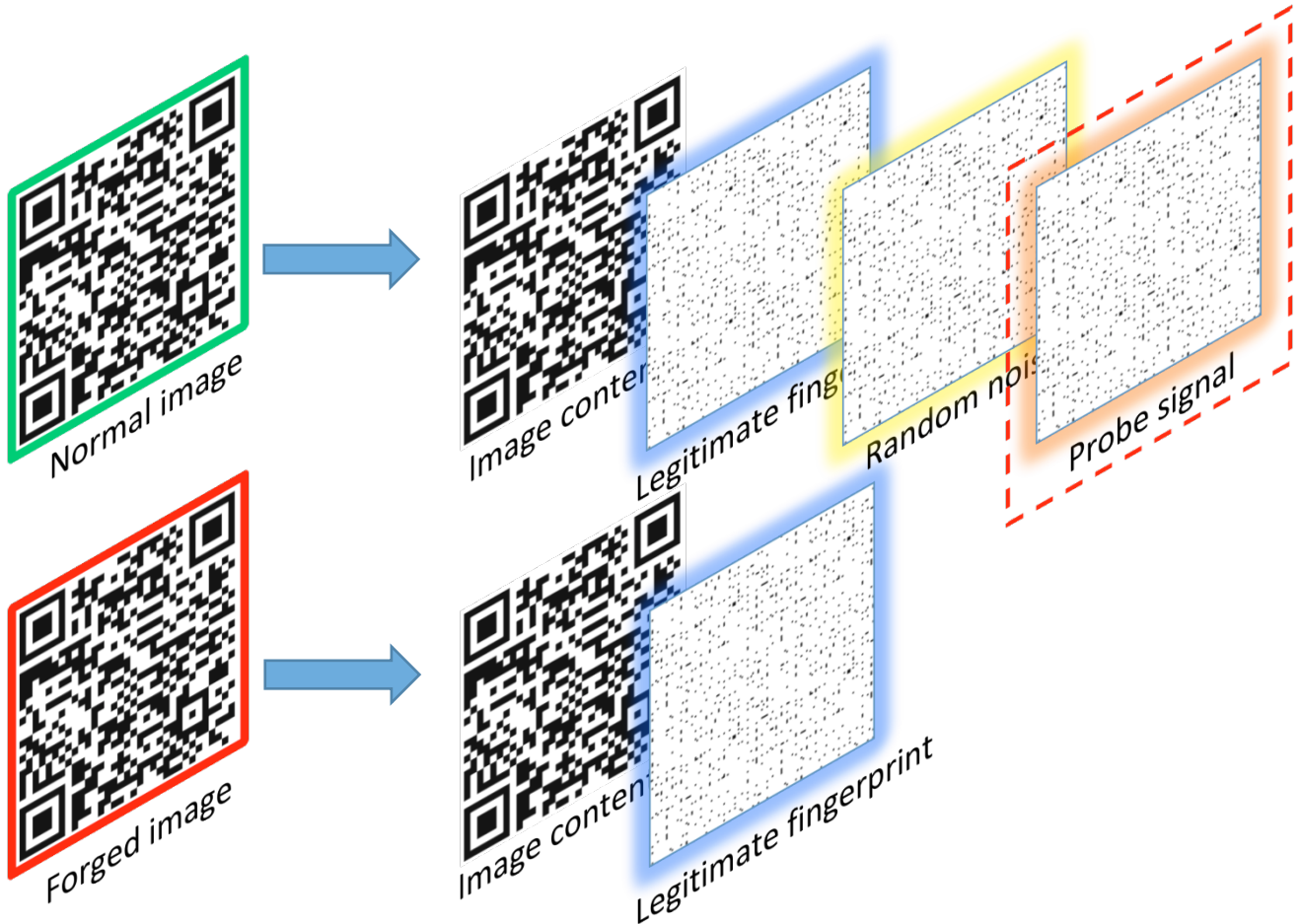
Solution: Probe Signal

- Embed a probe signal that will be removed by the fingerprint removal process



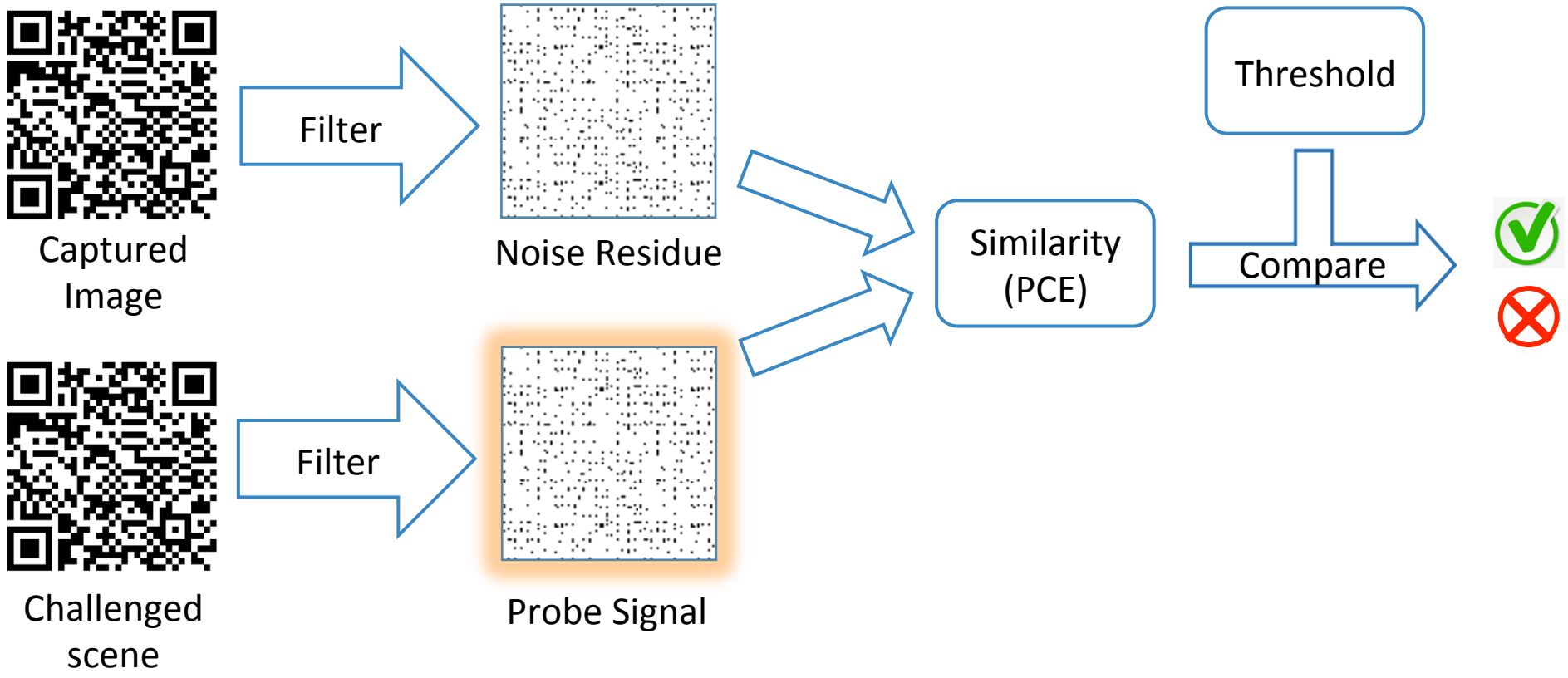
Solution: Probe Signal

- Detect removal attacks by checking the existence of the probe signal



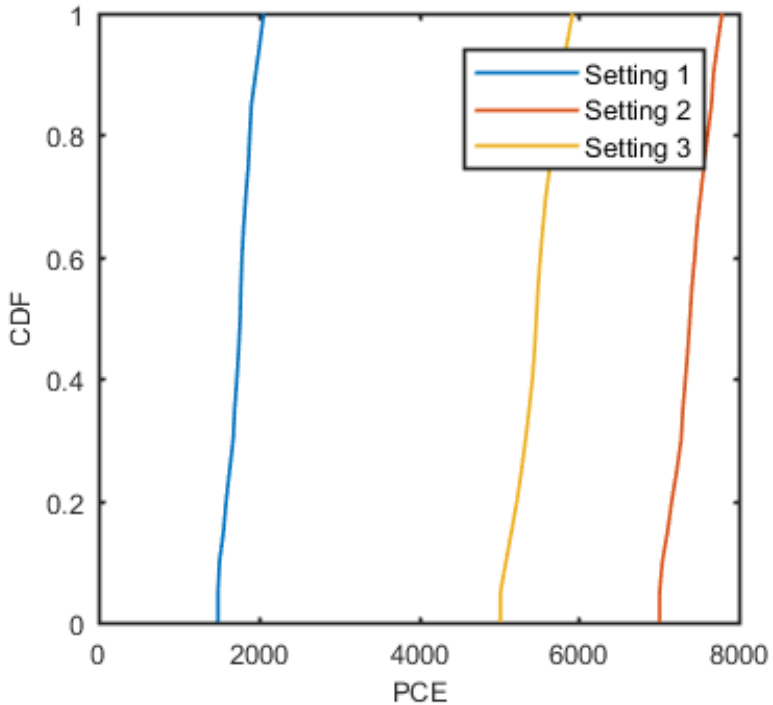
Solution: Probe Signal

- Detect removal attacks through checking the existence of the probe signal



Effectiveness of Removal Detection

- Setting 1: Target scene have no probe signal.
- Setting 2: Target scene have a probe signal. Normal Image.
- Setting 3: Target scene have a probe signal. Removal Attack.

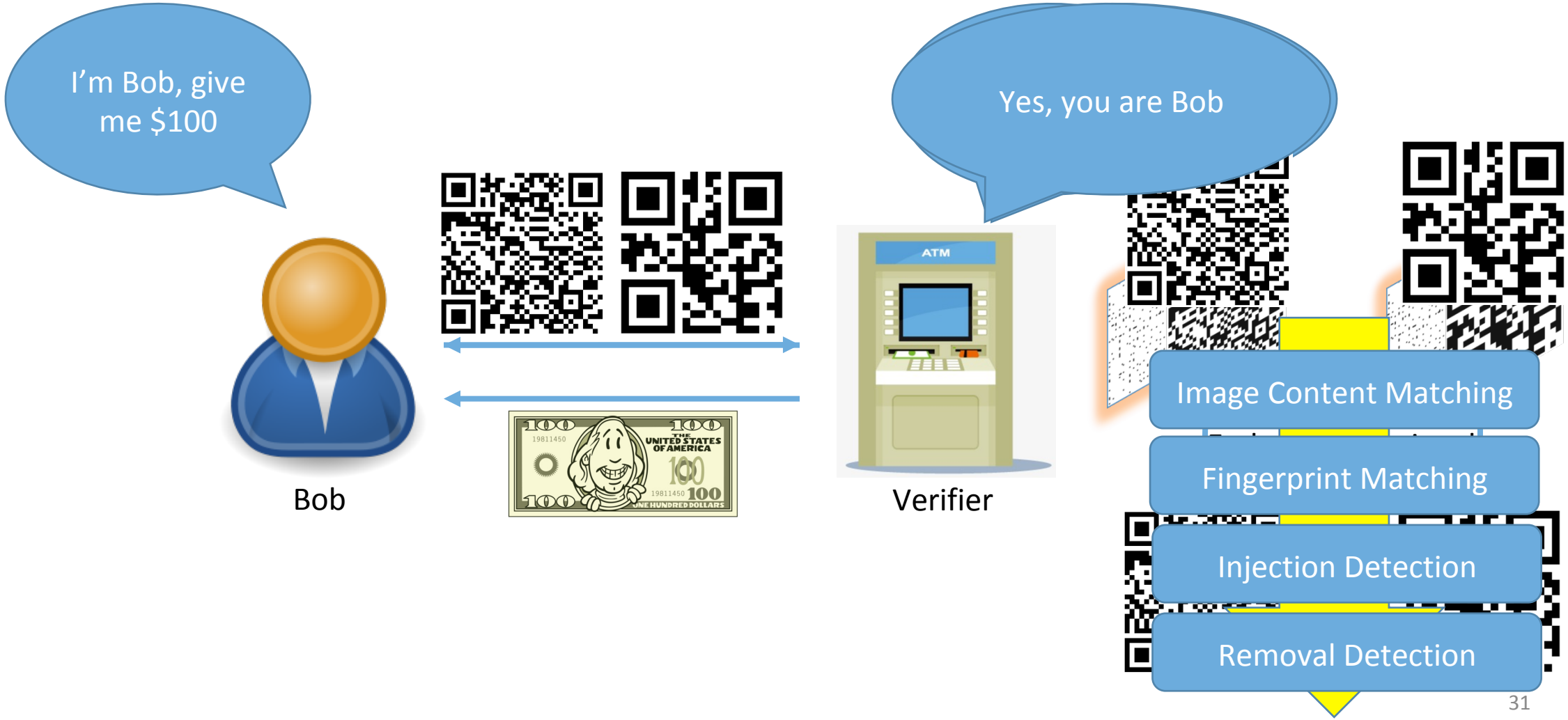


1. The probe signal is preserved in legitimate image tokens. (Setting **1** VS Setting **2**)

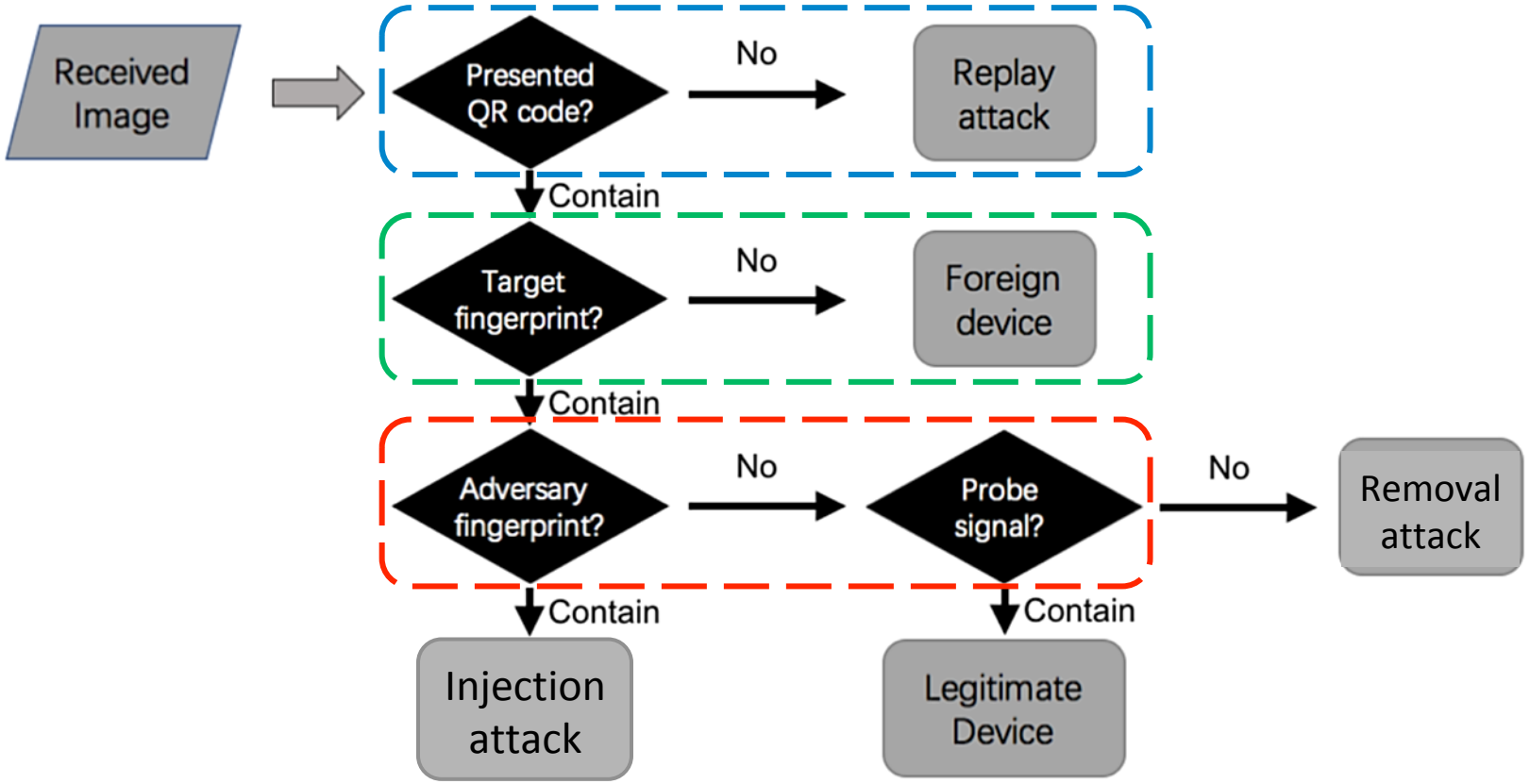
2. The probe signal is suppressed in forged images. (Setting **2** VS Setting **3**)

Forged images can be easily detected

Full-fledged Authentication Protocol



The Attack Detection Flow



Fingerprint leakage resilience

Reliable camera identification

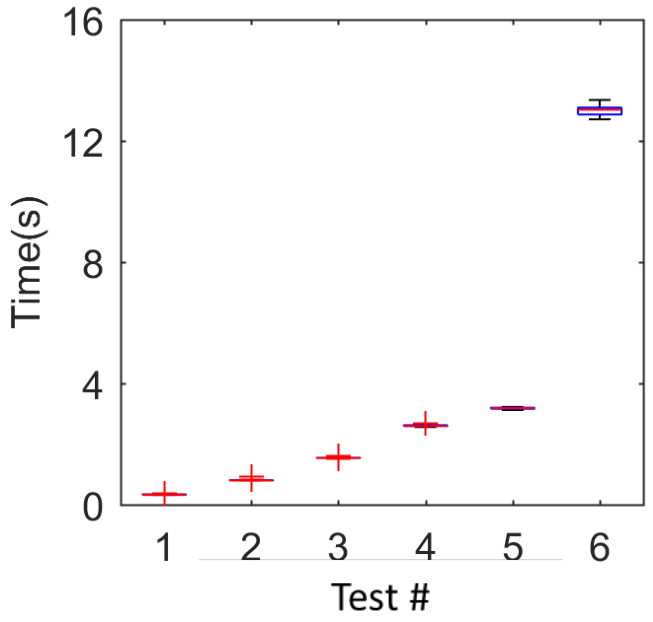
Fingerprint forgery Resilience

Efficiency

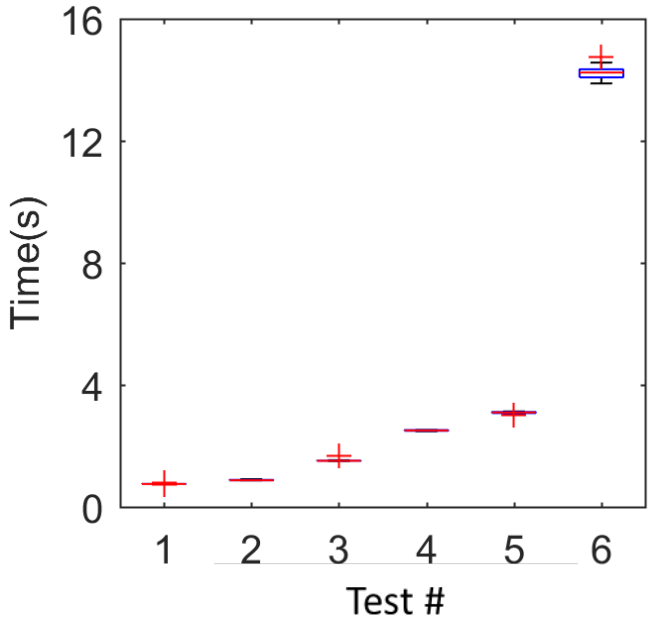
- Image Content Matching:
  - Determined by the version of the applied QR code. Normally can be finished within 0.1 second.
- Fingerprint Matching:
  - Determined by the resolution of the captured image. This is the most time consuming part.
- Injection Detection:
  - Determined by the resolution of the captured image. Normally can be finished within 0.5 second.
- Removal Detection:
  - Determined by the resolution of the probe signal. It takes at most 0.9 second.

Efficiency

Test#	1	2	3	4	5	6
Image Resolution	640x480	960x720	1280x960	1600x1200	2048x1152	3264x2448
Probe Resolution	200x200	200x200	400x400	400x400	400x400	800x800



Fingerprint Matching



Overall Efficiency

What Factors can Influence PRNU?

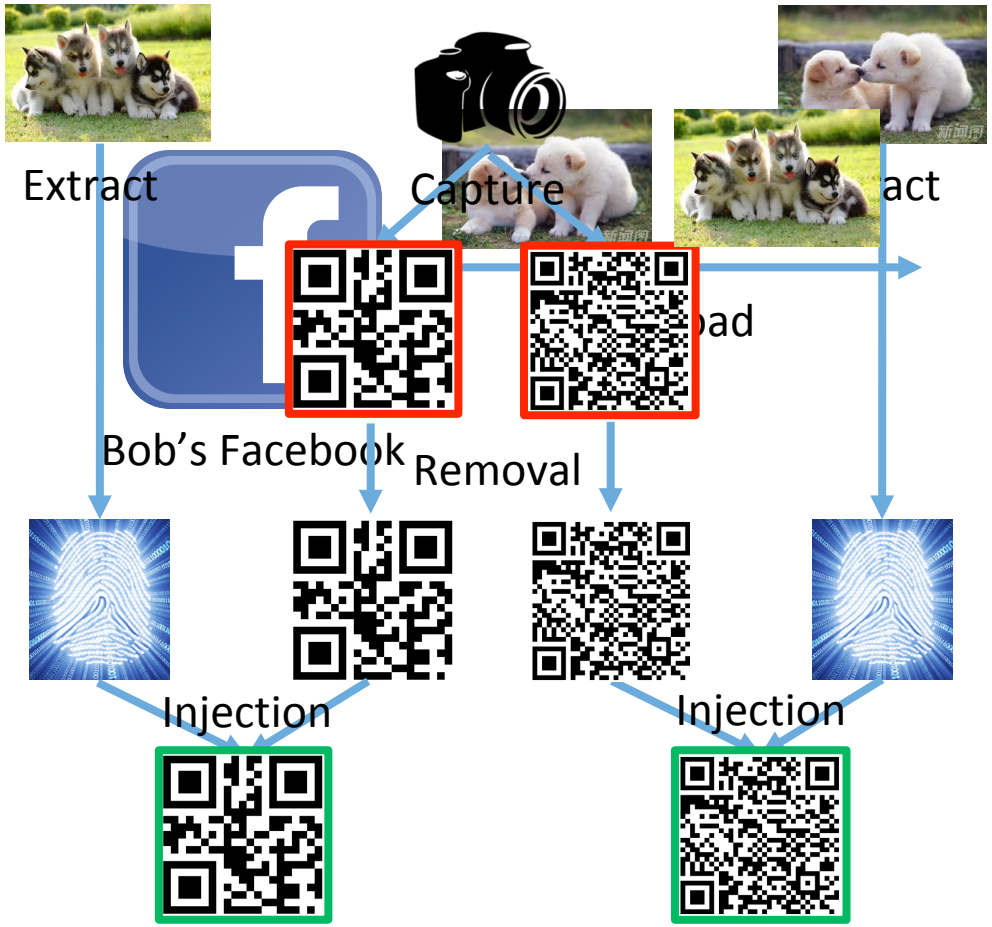
- Does PRNU change over time?
  - No
- Will the ambient environment affect the fingerprint on an image?
  - Only ambient light intensity.
- What is the relationship between an image's resolution and the strength of its fingerprint?
  - Positively correlated

Conclusion

- The first work to enable smartphone authentication using built-in camera
  - Accurate and efficient identification
  - Resilient to fingerprint leakage and forgery

Thank you! Questions?

Reinforced Fingerprint Forgery: the Removal Attack



Adversary

Verifier