Poster: Recovering Fingerprints from In-Display Fingerprint Sensors via Electromagnetic Side Channel

Tao Ni
City University of Hong Kong
taoni2-c@my.cityu.edu.hk

Xiaokuan Zhang
George Mason University
xiaokuan@gmu.edu

Qingchuan Zhao
City University of Hong Kong
qizhao@cityu.edu.hk

Title: Recovering Fingerprints from In-Display Fingerprint Sensors via Electromagnetic Side Channel

Authors: Tao Ni, Xiaokuan Zhang, Qingchuan Zhao

Venue: The 30th ACM SIGSAC Conference on Computer and Communications Security (CCS), Copenhagen, Denmark, 2023.

DOI: 10.1145/3576915.3623153

Full Reference [1]: Tao Ni, Xiaokuan Zhang, and Qingchuan Zhao. 2023. Recovering Fingerprints from In-Display Fingerprint Sensors via Electromagnetic Side Channel. In Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security (CCS'23). Association for Computing Machinery, New York, NY , USA, 253–267. https://doi.org/10.1145/3576915.3623153

Abstract: Recently, in-display fingerprint sensors have been widely adopted in newly-released smartphones. However, we find this new technique can leak information about the user's fingerprints during a screen-unlocking process via the electromagnetic (EM) side channel that can be exploited for fingerprint recovery. We propose FPLogger to demonstrate the feasibility of this novel side-channel attack. Specifically, it leverages the emitted EM emanations when the user presses the in-display fingerprint sensor to extract fingerprint information, then maps the captured EM signals to fingerprint images and develops 3D fingerprint pieces to spoof and unlock the smartphones. We have extensively evaluated the effectiveness of FPLogger on five commodity smartphones equipped with both optical and ultrasonic in-display fingerprint sensors, and the results show it achieves promising similarities in recovering fingerprint images. In addition, results from 50 end-to-end spoofing attacks also present FPLogger achieves 24% (top-1) and 54% (top-3) success rates in spoofing five different smartphones.

Paper Link: https://doi.org/10.1145/3576915.3623153

NDSS 2025 Poster Submission Type: Type 2: Recently Published Research

References

[1] T. Ni, X. Zhang, and Q. Zhao, "Recovering fingerprints from in-display fingerprint sensors via electromagnetic side channel," in *Proceedings of the ACM SIGSAC Conference on Computer and Communications Security (CCS)*, 2023.

Recovering Fingerprints from In-Display Fingerprint Sensors via Electromagnetic Side Channel

Tao (Tony) Ni[*], Xiaokuan Zhang[†], Qingchuan Zhao[*] **(Accepted by CCS'23)**

taoni2-c@my.cityu.edu.hk, qizhao@cityu.edu.hk [*]Department of Computer Science, City University of Hong Kong
xiaokuan@gmu.edu [†]Department of Computer Science, College of Engineering and Computing, George Mason University

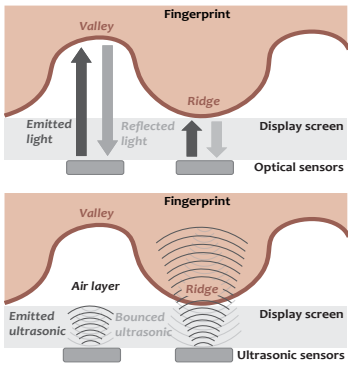
1. Introduction

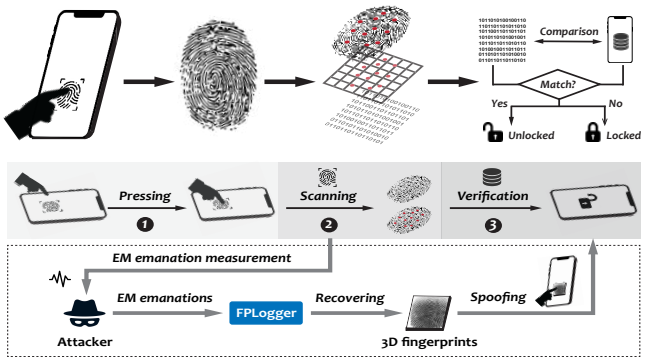
In-display fingerprint sensors are increasingly used in new smartphones. However, they can unintentionally reveal fingerprint data through electromagnetic (EM) emanations during the unlocking process. We introduce FPLogger to showcase the feasibility of this side-channel attack, which captures EM signals emitted when the sensor is pressed, then reconstructs fingerprint images and creates 3D models to spoof and unlock the device.

⚠ **Demo:** You can try to attack this smartphone (i.e., OnePlus 10 Pro) using the 3D fingerprint pieces reconstructed from FPLogger.

2. In-Display Fingerprint Sensors & Smartphone Authentication

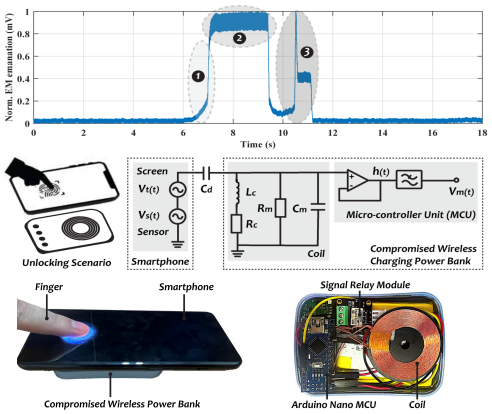
An optical or ultrasonic fingerprint sensor (e.g., Synaptics' Clear ID) is embedded beneath the LCD/OLED touchscreen, typically located on the bottom. When a user places their finger on the designated area of the screen, the thin-film transistor (TFT) array of the in-display fingerprint sensor emits either light from the backlight or ultrasonic waves generated from piezoelectric effect to scan the fingerprint and capture an image of the distinctive *ridges* and *valleys* on the fingerprint pattern. Then, the bounced light or ultrasonic signals are converted to pixel-cell electric currents that represent the signal strength in the gray-scale bitmap, which generates a contour image to describe the fingerprint. Finally, the generated fingerprint image will be compared to the stored fingerprint data to determine whether the user is authorized to unlock the device.





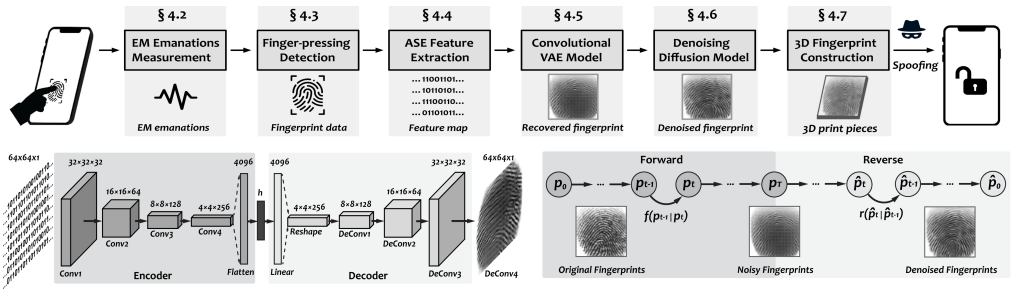
3. Electromagnetic (EM) Leakage

FPLogger leverages the coil in a compromised wireless charging power bank to capture the EM emanations during an unlocking process.



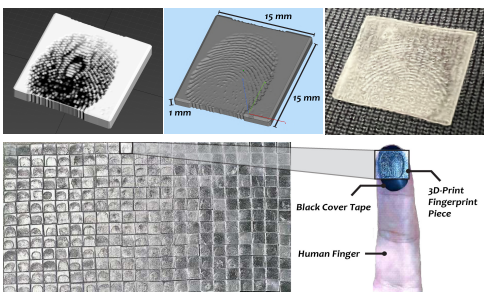
4. FPLogger Overview

FPLogger workflow: ❶ Capture EM emanations during a screen-unlocking action, ❷ Signal processing and fingerprint part segmentation, ❸ Adaptive-selected envelope (ASE) feature extraction, ❹ CVAE to map features to 2D fingerprint images, ❺ Denoising diffusion model to enhance fingerprint resolution, ❻ 3D fingerprint reconstruction and in-display sensor spoofing.



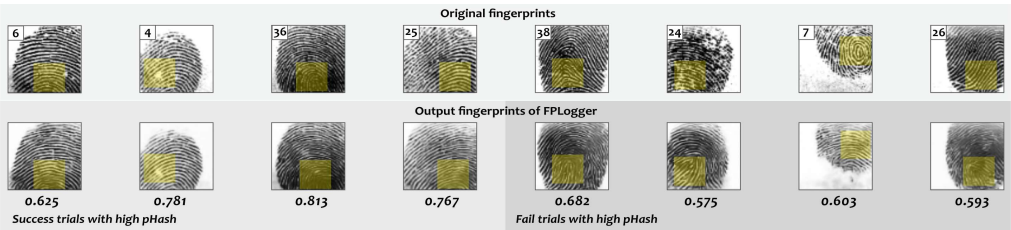
5. 3D Fingerprint Pieces

3D fingerprints construction from 2D images with 3ds Max, Materialise Magics, 3D printers.



6. Recovered Fingerprints with pHash Similarities

Illustration of eight end-to-end attack trials with high pHash similarity. Four successfully spoof the in-display fingerprint sensor, while the others do not. Yellow boxes: Similar/mispredicted patterns.



More details

For more details and recent progresses, you scan the QR codes below to read our CCS'23 paper and watch real-world attack demos.

Paper

Project & Demo

7. End-to-end Attacks on Real Registered Fingerprints

Smartphone	Register FP *dpi*	Test FP *dpi*	T-3 Results of Five Real Fingerprints													
			FP 1			FP 2			FP 3			FP 4			FP 5		
OnePlus 10 Pro	300–363	64	○	○	●	○	○	○	○	○	●	○	○	○	○	○	○
OPPO A96	300–363	64	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Redmi K20 Pro	300–363	64	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○
Huawei P30 Pro	300–363	64	○	○	○	○	○	○	○	○	●	○	○	○	○	○	○
Samsung S10	550	64	○	○	○	○	○	○	○	○	○	○	○	○	○	○	○