Poster: Sensor-based Vehicle Image Authentication

Zhilin Gao, Haoting Shen*, and Kui Ren
The State Key Laboratory of Blockchain and Data Security; Zhejiang University;
ZJU-Hangzhou Global Scientific and Technological Innovation Center
htshen@zju.edu.cn

***Abstract*—Trustable and reliable image capturing is critical to ensure the security of autonomous driving and driver assistance systems. It requires the image is captured by the authorized sensor as it is claimed and the image content is intact. However, such authentication techniques adaptable on practical vehicle image sensors are still in a lack. Here we propose an in-sensor physical unclonable function (PUF) design for reliable sensor sourcing and image content authentication. The design exploits the unique self-discharging behavior of each sensor pixel's capacitive well structure.**

Background. During autonomous driving, environment images are continuously captured by the on-vehicle sensors and processed by the on-vehicle processing unit, such that proper driving actions can be performed by the control system. A successful injection of images from manipulated sources or tampered images can result in serious damages. Countermeasures, such as digital signature based on asymmetric encryption or AI-enhanced image authentication, come with limitations on vehicles for reasons, including the sensors' limited computing resource and advanced content generation techniques.

PUF-design. Previously, a PUF-based image authentication design was proposed for the authentication of image sourcing camera and image integrity in [1], where the fixed pattern noise (FPN) of sensor pixels was used to build the PUF module. Since FPN is sensitive to the environmental light, a mechanical shutter shielding the sensor is thus necessary to allow the PUF to work correctly. However, such a mechanical structure is typically not available in compact vehicle image sensors. Here we propose a new in-sensor PUF design based on the capacitive well structure in pixels (highlighted by red frame in Fig. 1a).

The well structure can be covered by masking materials. When the gate TX in Fig. 1a is set off, the well structure is isolated from the light impacted area, making it insensitive to environmental light and hence can be applied on vehicle image sensors. Transistor T1 is used to control the charging of the capacitive well, while the discharging occurs through surrounding circuits. Due to the variation during the manufacturing process, the discharging rates of different pixels are slightly and randomly differ. Such behaviors are used to build the PUF. Image features are extracted to serve as PUF challenges and the well discharging rate comparing results are used for PUF responses. The authentication tag generation are depicted in Fig. 1b.

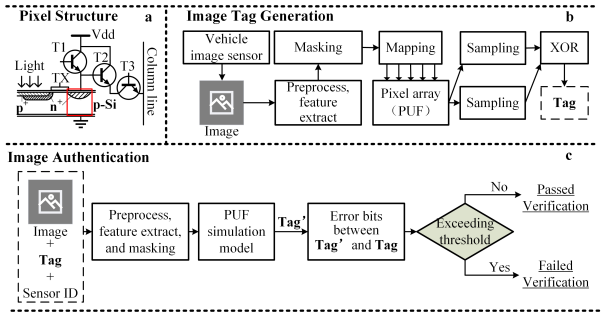

Fig. 1. Schematic diagram of proposed image authentication solution

Authentication. Each image from the sensor is verified with the corresponding tag and sensor ID. As comparing to tampering, the benign altering of extracted feature is typically within a small range, we compare the bit error rate of each DCT block feature and use the highest value among them as the basis for judgment. (Fig. 1c).

Experiments. Device-level capacitive well discharging simulation results, tampered image authentication and falsely claimed source authentication results are described in Fig. 2a,b and c, respectively. Data set used here is from [2].

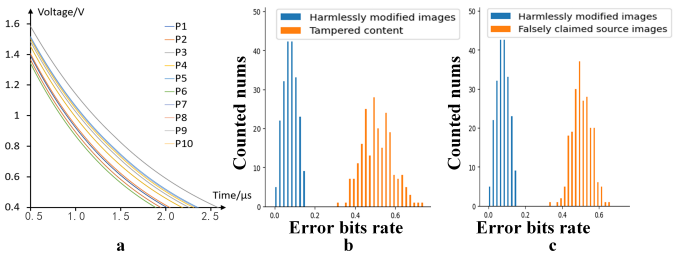

Fig. 2. Experimental results.

References

[1] Y. Zheng, Y. Cao and C. H. Chang, A PUF-based Data-device Hash for Tampered Image Detection and Source Camera Identification. In IEEE Transactions on Information Forensics and Security, vol. 15, pp. 620-634, 2020.

[2] P. Korus and J. Huang, Multi-scale Analysis Strategies in PRNU-based Tampering Localization, IEEE Trans. Information Forensics and Security, 2017

Symposium on Vehicles Security and Privacy (VehicleSec) 2024
26 February 2024, San Diego, CA, USA
ISBN 979-8-9894372-7-6
https://dx.doi.org/10.14722/vehiclesec.2024.2510
www.ndss-symposium.org