Smartphone Authentication Using PRNU

Shinoy Yandra, Ashwin Sabu, Adithya Nair, ASV Prasasya

*Computer Science and Engineering)*

*Amrita School of Computing, Amrita Vishwa Vidyapeetham.)*

Amritapuri, India

***Abstract***—

***Literature review.***

***Papers reviewed:***

* ABC: Enabling Smartphone Authentication with Built-in Camera. Zhongjie Ba, Sixu Piao, XinwenFu, Dimitrios Koutsonikolas, Aziz Mohaisen and Kui Ren. University at Buffalo, State University of New York on 25th Annual Network and Distributed System Security Symposium, NDSS 2018
* CHEN, S., REN, K., PIAO, S., WANG, C., WANG, Q., WENG, J., SU, L., AND MOHAISEN, A. You can hear but you cannot steal: Defending against voice impersonation attacks on smartphones. In Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on (2017), IEEE, pp. 183–195.
* CHEN, M., FRIDRICH, J., GOLJAN, M., AND LUKAS´, J. Determining image origin and integrity using sensor noise. IEEE Transactions on Information Forensics and Security 3, 1 (2008), 74–90.
* CHEN, M., FRIDRICH, J., AND GOLJAN, M. Digital imaging sensor identification (further study). In Electronic Imaging 2007 (2007), International Society for Optics and Photonics, pp. 65050P–65050P
* BOJINOV, H., MICHALEVSKY, Y., NAKIBLY, G., AND BONEH, D. Mobile device identification via sensor fingerprinting. arXiv preprint arXiv:1408.1416 (2014).
* BRIK, V., BANERJEE, S., GRUTESER, M., AND OH, S. Wireless device identification with radiometric signatures. In Proceedings of the 14th ACM international conference on Mobile computing and networking (2008), ACM, pp. 116–127.
* LUKAS, J., FRIDRICH, J., AND GOLJAN, M. Digital camera identification from sensor pattern noise. IEEE Transactions on Information Forensics and Security 1, 2 (2006), 205–214.
* POLAK, A. C., DOLATSHAHI, S., AND GOECKEL, D. L. Identifying wireless users via transmitter imperfections. IEEE Journal on Selected Areas in Communications 29, 7 (2011), 1469–1479.
* POLAK, A. C., DOLATSHAHI, S., AND GOECKEL, D. L. Identifying wireless users via transmitter imperfections. IEEE Journal on Selected Areas in Communications 29, 7 (2011), 1469–1479.
* BA, Z., AND REN, K. Addressing smartphone-based multi-factor authentication via hardware-rooted technologies. In Distributed Computing Systems (ICDCS), 2017 IEEE 37th International Conference on (2017), IEEE, pp. 1910–1914.

* DAS, A., BORISOV, N., AND CAESAR, M. Do you hear what i hear? Fingerprinting smart devices through embedded acoustic components. In Proceedings of the 2014 ACM SIGSAC Conference on Computer and Communications Security (2014), ACM, pp. 441–452.

In each paper, we used for Literature review the most pronounced thoughts are put upon the word SECURITY. Under each document, they proposed various methods for various security-related issues.

The author Zhongjie Ba came up with an idea on ABC, a real-time smartphone Authentication protocol that leverages the built-in-camera’s Photo-Response Non-Uniformity (PRNU). In contrast to a previous study that required hundreds of images to create a reliable PRNU feature for conventional cameras, researchers are the first to observe that one image alone can uniquely identify a smartphone due to the unique PRNU of a smartphone image sensor. The new discovery makes the use of PRNU practical for smartphone authentication. ABC defeats, forgery attacks by verifying a smartphone’s PRNU identity using a visible light communication channel. A user captures two time-variant QR codes and sends the two images to a server, which verifies the identity by fingerprint and image content matching. The time variant QR codes can also mitigate replay attacks. They experiment with several images with various smartphones. show that ABC can efficiently authenticate user devices with an error rate less than 0.5%.

The authors came up idea in identifying the camera by which an image is taken is given by analyzing the PRNU of a camera sensor which will be unique to its sensor and can be determined which intern can be used against the PRNU in the dataset available to find the camera sensor by which the image is taken. For finding the PRNU various methodologies were used. They used the co-relation scores of the input image and the images kept earlier to find out the sensor used. If the score is higher, the chance for it to be of the same sensor is higher and vice-versa.

The author CHEN, S explained about the voice impersonation in devices. which means acting out as a different person by using their sound to exploit other's devices. Particularly on small mobile devices like smartphones and smartwatches, voice offers a considerable advantage over the traditional keyboard-based input methods in terms of convenience and efficiency. However, because the human voice is frequently made available to the public, an attacker can easily record sound samples from their intended victims before launching voice impersonation assaults to fool such voice-based applications. The design and implementation of a strong software-only voice impersonation defensive system that is suited for mobile platforms and is simple to interface with current off-the-shelf smart devices are proposed in the study. They investigate the magnetic field emitted from loudspeakers as the key property for identifying attacks using automated voice imitation. Furthermore, to protect against human impersonation attacks, they used a cutting-edge automatic speaker verification system. The system that they employed showed 100% perfection in finding the impersonation attacks and with 0% error.

CHEN, M. and FRIDRICHAND determining the image's origin and its integrity. Using PRNU, which is a distinctive fingerprint of imaging sensors, they used a unified framework for determining the source digital camera from its photos and for detecting digitally manipulated photographs. A simplified model of the sensor output is used to derive the PRNU using an estimator. By finding instances of sensor PRNU in particular areas of the image under inspection, objectives are subsequently accomplished. A testing problem is used to frame the detection. By employing a predictor of the test statistics on small image counts, the statistical distribution of the ideal test statistics is determined. The predictor makes it possible to estimate probabilities of incorrect rejection of a correct camera and missed detection of a tampered region more accurately and meaningfully. Furthermore, they provide a benchmark implementation of this framework and a thorough experimental validation. The proposed forensic techniques' resilience is evaluated using standard image processing techniques such as JPEG compression, gamma correction, scaling, and denoising.

BOJINOV came up with an idea that fingerprinting system uses the speakers to emit a sequence of sounds at different frequencies and records the resulting signals using the microphone. The finger printing is computed by looking at the amplitude and frequency distributions in the record signals and it also uses the accelerometer it measures forces in each of the three dimensions. Imprecisions in accelerometer calibration errors by solving an optimization problem and using the resulting six values as a fingerprint.

The author BRIK proposed a wireless device identification via radiometric signatures the best results achieved when all the metrics are combined together the frequency error, sync correlation, magnitude error and phase error. This classification accuracy can be improved if it is performed on multiple frames, rather than just one. In this paper we have addressed the fundamental issue of wireless NIC identification at the physical layer. We designed and implemented; a technique that identifies wireless transmitter devices based on minor artifacts in their emissions that are produced by distinctive hardware properties of individual NICs.

LUKAS proposed a model on Digital camera identification from pattern noise, there are numerous sources of imperfections and noise that enter into various stages of the image acquisition process. The two main components of the pattern noise are the fixed pattern noise (FPN) and the photo response non uniformity noise (PRNU). The fixed pattern noise is caused by dark currents. Fixed pattern noise also depends on exposure and temperature. The PRNU is classified into PNU and Low frequency defects.

POLAK came up with an idea in Identifying wireless users via transmitter imperfections, to tie criminal transmissions of a user to other transmissions of that same user. Radio frequency approach exploits channel information. In this paper there were two main components the digital-to-analog converter (DAC) and the power amplifier (PA). In this paper a new approach based on minute imperfections of different components of the transmitter hardware has been proposed for breaking user anonymity in wireless communication systems. The general models used to model the transmitter components allow for the determination of the probability of error of the decisions, which makes the proposed methods especially interesting for

establishing probable cause and for use in court. simulations have shown that the nonlinear variations of digital to analog converters can only be exploited when the signal to noise ratio is relatively high. However, in case of power amplifiers measurements from commercially employed chips indicate that amplifiers can be easily identified at typical power levels even at low SNRs and with very short observed sequences.

Researches like BA, Z., AND REN, K proposed a technique that improves the security of users’ sensitive data with the help of multi-factor authentication. The user must correctly demonstrate two or more authentication elements, such as knowledge, possession, and inherence factors, in order to successfully authenticate themselves.

For smartphone-based multi-factor authentication, a promising way to authenticate a user is to verify his possession of a legitimate smartphone, which ensures secure and usable device authentication schemes. In the article, they proposed to authenticate a device through tracking the hardware fingerprint of its built-in sensor.

Initially, they reviewed the existing hardware-rooted identification methods and discussed the merits of applying a hardware fingerprint as a smartphone's unique identity. Then, they analyzed the security issues underlying these methods and identified two security requirements for the identification methods to be used in an authentication scheme: Fingerprint Leakage Resilience and Fingerprint Forgery Resilience. Finally, they looked into a specific hardware fingerprint originally used for digital cameras. They analyzed the feasibility of applying this fingerprint to differentiate off-the-shelf smartphones and list several challenging practical issues underlying this method.

**Research Challenges, Open issues, Research Gap:**

The research challenge ahead is to get the PRNUs of both the input images and testing images and correlates it to the PRNU of the image input to get the output. The environmental factors also effecting the camera fingerprint. The main factor is intensity of ambient light.so, it is too difficult to find the PRNU of an image from the same camera in outdoor and indoor images which can have different PRNUs. so, the correlation will be difficult and strength of the fingerprint on an image significantly increases with the rise of the ambient light intensity

The research gap found here is to use Dark Signal Non-uniformity (DSNU) along with Photo response Non-Uniformity (PRNU) to determine the image sensor. Furthermore, it can be used to make a protocol which uses this technology to authenticate the user in any kind of IoT device. Nowadays, many smartphone manufacturers adopting a dual-camera system, researchers plan to investigate how to take advantage of the extra camera and improve the security of ABC as future work. With a dual-camera system, the verifiers will be able to identify each smartphone with fingerprints of the two cameras and further increase the difficulty of fingerprint forgery

**Dataset:**

Here, we used image sets include 275 images captured by vivo Y51 mobile and 275 images captured by Samsung Galaxy S21 mobile. And for testing we used image sets include 478 images. The resolution of the vivo Y51 images and Samsung S21 images are 640 x 352, 640x352 respectively.

**Proposed Approach:**

To verify the effectiveness of the PRNU fingerprint of a smartphones we collected 275 images from the two smartphones. With the help of the MATLAB code, we find the reference PRNU and then correlates between the test PRNU and the reference PRNU. We use Peak Correlation Energy (PCE) which is the most used similarity metric, for identifying the smartphone. PCE is defined as the ratio between the height of the peak and the energy of the cross correlation between reference PRNU and the obtained PRNU patterns

**PRNU-based camera Fingerprinting:**

PRNUis caused by an image sensor’s non-uniform sensitivity to light. It introduces a multiplicative factor to the actual optical view.

Any image captured by a digital camera can be represented as

**I = I (0) + I (0)K +** θ

Where, ‘I’ is the real sensor output and ‘I (0)’ denotes the actual optical view

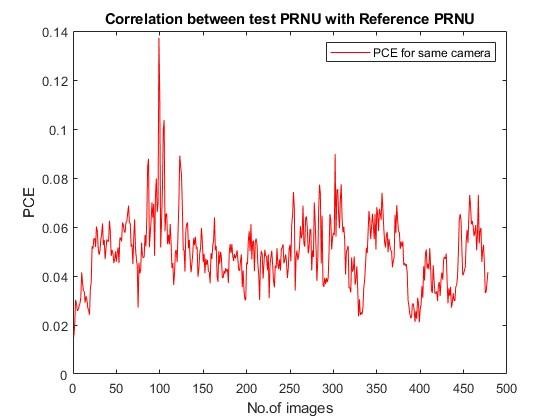
K is the camera’s PRNU, and θ represents other noise components

Since PRNU behaves like a white Gaussian noise variable with a variance and it can be extracted using a denoising filter. The extracted noise residual ‘W’ can be represented as

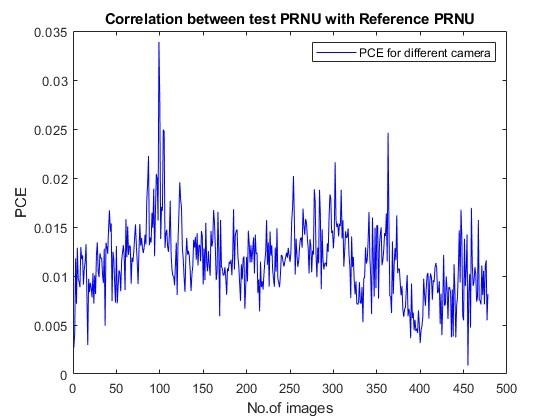
**W = I\*K + έ**

Where έ is a random noise component combining θ and other minor components

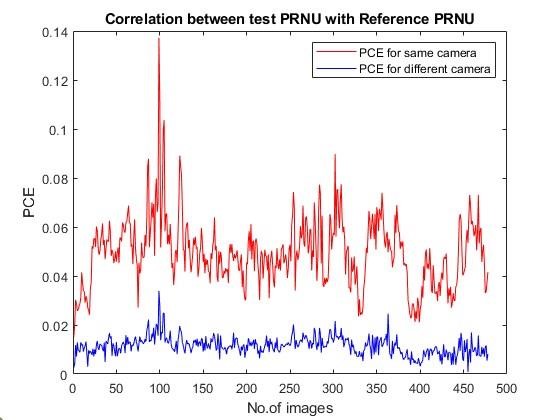
We use the following approach to evaluate the fingerprint of a smartphone camera. Peak to Correlation Energy (PCE) measures the correlation between an unknown image’s noise residual and the reference fingerprint.



The above figure shows the correlation between the reference PRNU obtained by Vivo Y51 camera and unknown images (test PRNU)



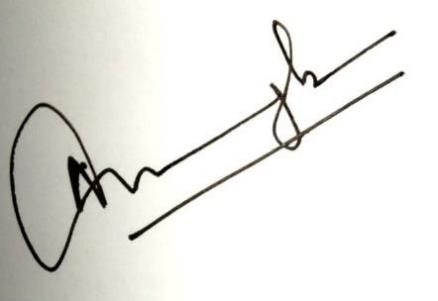
The above figure shows the correlation between the reference PRNU obtained by Samsung S21 camera and unknown images (test PRNU)



From this figure we can say that both vivo Y51 and Samsung S21, images taken same smartphone shows significantly higher correlation than images captured by the different smartphone. From this we can conclude that the unknown images/test images are also taken from vivo Y51 camera.

**References:**

1. https://par.nsf.gov/biblio/10084235-abc-enabling-smartphone-authentication-built-camera
2. https://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=9656877
3. https://www.researchgate.net/publication/303912935\_Leveraging\_Sensor\_Fingerprinting\_for\_Mobile\_Device\_Authentication
4. https://www.researchgate.net/publication/220926608\_Wireless\_device\_identification\_with\_radiometric\_signatures
5. https://www.researchgate.net/publication/3455253\_Digital\_Camera\_Identification\_From\_Sensor\_Pattern\_Noise
6. https://www.researchgate.net/publication/224249899\_Identifying\_Wireless\_Users\_via\_Transmitter\_Imperfections
7. https://www.researchgate.net/publication/285221309\_Wireless\_Device\_Authentication\_Using\_Acoustic\_Hardware\_Fingerprints
8. https://www.researchgate.net/publication/228590993\_Digital\_imaging\_sensor\_identification\_further\_study\_-\_art\_no\_65050P
9. https://www.researchgate.net/publication/318476509\_You\_Can\_Hear\_But\_You\_Cannot\_Steal\_Defending\_Against\_Voice\_Impersonation\_Attacks\_on\_Smartphones
10. https://www.researchgate.net/publication/3455393\_Determining\_Image\_Origin\_and\_Integrity\_Using\_Sensor\_Noise



Nimmy K