Forensic Insights from iPhones using EM-SCA

Lojenaa Navanesan, Kasun De Zoysa, and Asanka Sayakkara
University of Colombo School of Computing, Colombo, Sri Lanka.
University of Vavuniya, Vavuniya, Sri Lanka.
lojenaa@vau.ac.lk

1. Introduction

Digital forensics is essential for uncovering hidden details in criminal cases involving smart devices. Electromagnetic side-channel analysis (EMSCA) has been introduced and examined on specific smartphones and IoT devices to validate its usefulness in forensic investigations [1]. This study aim to gather a range of iPhones to verify the consistent effectiveness of EMSCA across similar devices. Despite initial challenges regarding compatibility, the implementation of transfer learning techniques led to better results, signifying significant progress. The study's expanding scope suggests its potential influence on future cross-device adaptation studies involving a variety of devices [2].

2. Background

The HackRF One SDR played a crucial role in capturing and analyzing EM radiation in smartphones [3]. This approach offers insights into software execution, benefiting digital forensics by reconstructing device activity timelines and unraveling the sequence of events leading to specific scenarios.

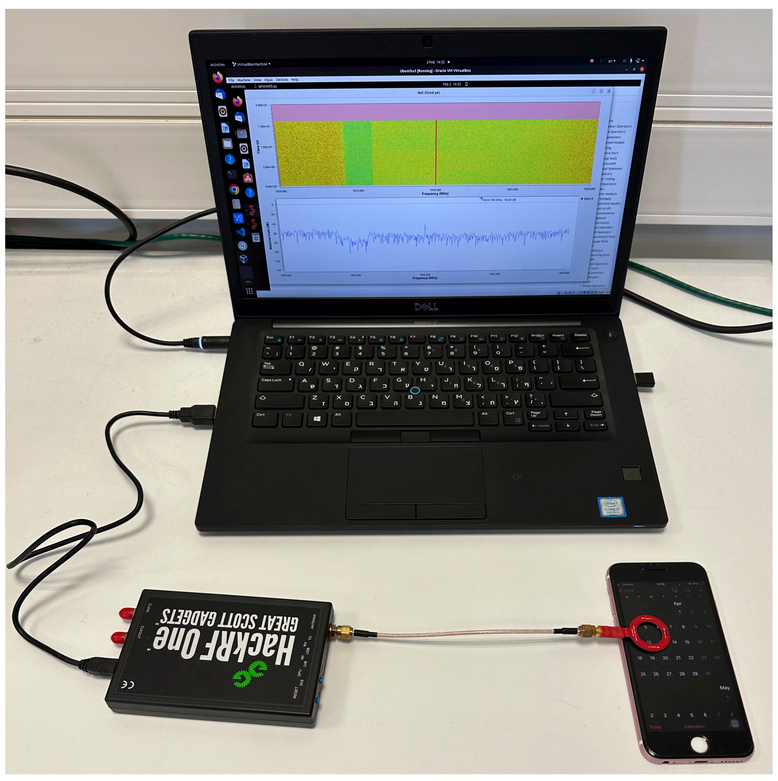

Figure 1: Four applications after performing PCA on their EM signals

4. Collected Devices

System-on-Chip	Architecture	CPU Frequency	Devices
Apple A5	ARMv7-A	1GHz (2 cores)	**iPhone 4S**
Apple A9	ARMv8-A	1.85GHz (2 cores)	**iPhone 6S**
Apple A11 Bionic	ARMv8-A	2.39GHz (6 cores)	**iPhone 8**
Apple A15 Bionic	ARMv8.5-A	3.23 GHz (6 cores)	**iPhone 13**
Apple A16 Bionic	ARMv8.6-A	3.46 GHz (6 cores)	**iPhone14 Pro**

Figure 3: Specifications about the devices targeted to capture EM trace files while ten different software activities were running on each of the chosen iPhones

5. Classification Model

Layer(type)	Output Shape	No. of Parameters
dense (Dense)	(None, 1400)	2868600
dense_1 (Dense)	(None, 800)	1120800
dense_2 (Dense)	(None, 500)	400500
dense_3 (Dense)	(None, 200)	100200
dense_4 (Dense)	(None, 100)	20100
dense_5 (Dense)	(None, 10)	1010

Figure 4: The layout of the current machine learning model employing the newly obtained dataset from smartphone

The model undergoes a 30-epoch training using an *opt* optimizer and sparse *categorical cross-entropy* loss function.

3. Methodology

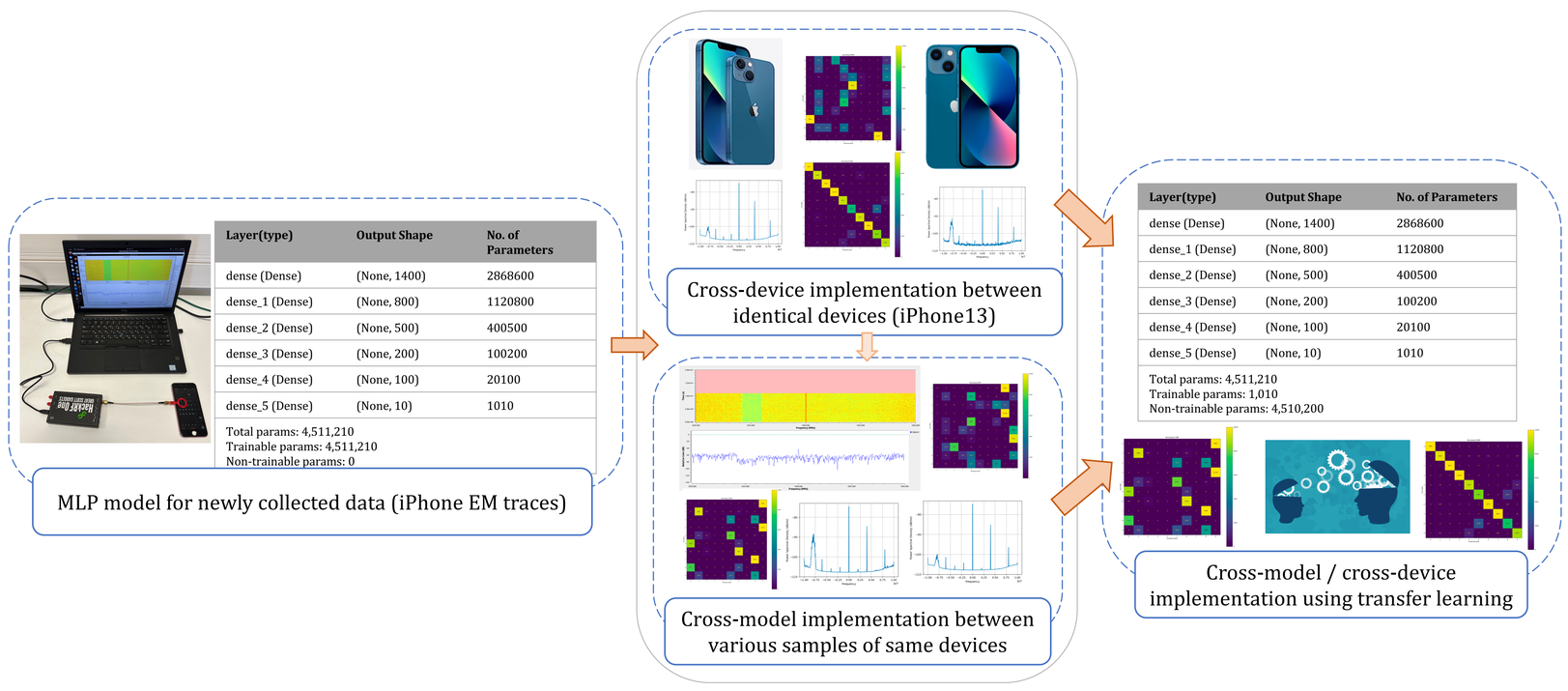

Figure 2: An elaborate flow diagram is employed to demonstrate the entire step-by-step procedure of the experiment involving the iPhone.

6. Results and Discussion

Figure 5 depicts the accuracy of new EM traces on different iPhone types using the EMSCA model, with an average accuracy of nearly 99% for each device.

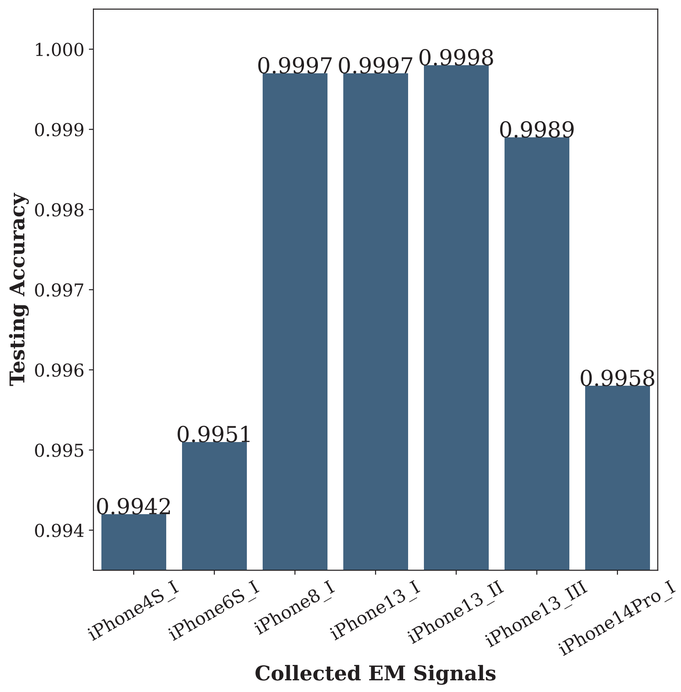

Figure 5: Implementation of the existing EMSCA model to determine the accuracy of various devices

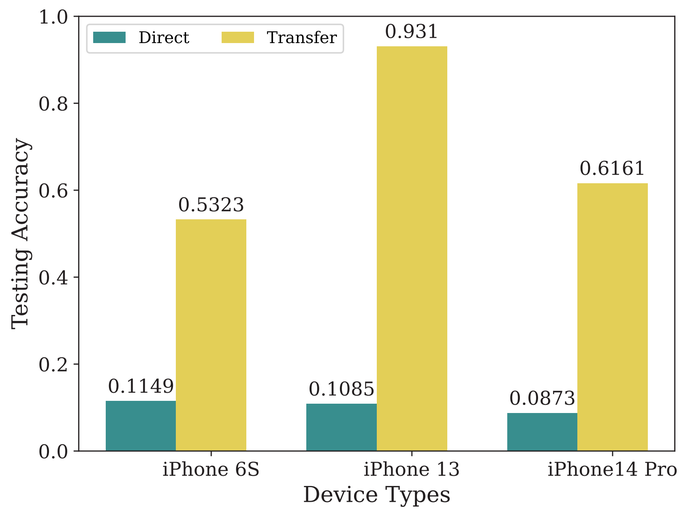

Figure 6: Direct machine learning accuracy versus transfer learning accuracy

Figure 6 outlines the assessment of accuracy between iPhone6S, 13, and 14Pro using both direct application of a pre-trained model to newly collected data and transfer learning via output layer training. The utilization of transfer learning demonstrates a notable improvement in accuracy compared to the direct pre-trained model.

7. Conclusion and Future Work

Cross-device implementation challenges are shown by the examination of EM traces from iPhones. Digital forensics on smart devices is facilitated by model performance and adaptability improvements using transfer learning.

Future Work:
Implementing noise cancellation on raw EM traces is a key strategy for enhancing accuracy in cross-device portability.

8. References

[1] Sayakkara et al. Electromagnetic side-channel analysis for iot forensics: Challenges, framework, and datasets. *IEEE Access*, 2021.

[2] Yu et al. Cross-device profiled side-channel attacks using meta-transfer learning. In *ACM/IEEE (DAC)*. IEEE, 2021.

[3] Sayakkara et al. Electromagnetic side-channel attacks: potential for progressing hindered digital forensic analysis. In *ISSTA/ECOOP*, 2018.