Computational Sensor Fingerprints

Paweł Korus, *Member, IEEE*, and Nasir Memon, *Fellow, IEEE*

***Abstract*— Analysis of imaging sensors is one of the most reliable photo forensic techniques, but it is increasingly challenged by complex image processing in modern cameras. The underlying photo response non-uniformity (PRNU) is distilled into a static sensor fingerprint unique for each device. This makes it easy to estimate and spoof and limits its reliability in face of sophisticated attackers. We propose to exploit computational capabilities of emerging intelligent vision sensors to design next-generation *computational sensor fingerprints*. Such sensors allow for running neural network inference directly on raw pixels, which enables end-to-end optimization of the entire photo acquisition and distribution pipeline. Control over fingerprint generation allows for adaptation to various requirements and threat models. In this study we provide a detailed assessment of security properties and evaluate two approaches to prevent spoofing: fingerprint generation based on local image content and adversarial training. We found that adversarial training is currently impractical, but content fingerprints deliver good performance in the considered cross-domain (RAW-RGB) setting and could provide robust best-effort protection against photo manipulation. Moreover, computational fingerprints can alleviate other limitations of PRNU, e.g., its limited reliability for dark/texture**

chronization between the analyzed image and the fingerprint which makes the process brittle and may require brute-force search for synchronization. While efficient algorithms exist for simple transformations (e.g., cropping) many post-processing steps need complex heuristics (e.g., motion-stabilized video [7] or high dynamic range imaging [8]) or have no solutions at all. Increasing adoption of computational photography and learned image processing operators will be another challenge. Problems with fingerprint uniqueness have already been reported for modern smart-phones [9] and neural image signal processors (ISPs), even trained to faithfully reproduce the standard camera pipeline, can yield incompatible fingerprints [10], [11]; more complex pipelines (e.g., for low-light imaging [12]) can invalidate the approach entirely [11]. As ISPs evolve, intrinsic sensor fingerprinting will likely become obsolete.

We believe computational photography brings not only challenges but also opportunities. We show that it is possible to learn novel sensor fingerprints using neural networks (NNs). Such *computational sensor fingerprints* (CSF) could be