proceedings

Proceedings

Efficient PRNU Matching in the Encrypted Domain †

Alberto Pedrouzo-Ulloa [1,*], Miguel Masciopinto [1], Juan Ramón Troncoso-Pastoriza [2] and Fernando Pérez-González [1]

[1] Theory and Communications Department, University of Vigo,36310 Vigo, Spain
[2] École Polytechnique Fédérale de Lausanne, School of Computer and Communication Sciences, CH-1015 Lausanne, Switzerland
* Correspondence: apedrouzo@gts.uvigo.es

† Presented at the 2nd XoveTIC, A Coruña, Spain, 5–6 September 2019.

Published: 31 July 2019

Abstract: Photoresponse Non-Uniformity (PRNU) is becoming particularly relevant within digital media forensics, as a means to effectively determine the source camera of a given image. Most of the practical applications in digital media forensics involve dealing with highly sensitive data whose content must be protected. In this context, several secure frameworks have been proposed to perform PRNU-based camera attribution while preserving the privacy of both the testing images and the PRNU fingerprint. The two most recent and relevant ones, independently proposed in 2018, are (a) Mohanty et al.'s, who combine the use of a trusted environment (ARM TrustZone) to compute the PRNU fingerprint, with the Boneh-Goh-Nissim (BGN) cryptosystem to perform the matching, and (b) Pedrouzo-Ulloa et al.'s, who propose a more flexible solution which can be fully implemented on a general purpose architecture and does not require access to a trusted environment. In this work, we revisit the existing frameworks and propose a general formulation for PRNU matching based on lattice cryptosystems which improves on the BGN-based solution in terms of efficiency, flexibility and privacy.

Keywords: Photoresponse Non-Uniformity; lattice-based cryptosystems; digital media forensics; camera attribution forensic analyzer

1. Introduction

Photoresponse Non-Uniformity (PRNU) is a specific noise pattern inherent to digital imaging sensors [1]. It is becoming especially relevant in digital media forensics as, due to its random nature, can be used as a fingerprint of the underlying device.

In particular, PRNU has a great protential within image forensics, as it can help to determine whether a given image was taken by a certain camera [2]. Actually, several commercial applications are already able to identify acquisition devices, but they present two apparently contradictory needs:

- *High Computational Demands:* Outsourcing is an appealing solution for digital media forencis because the involved operations are computationally intensive and they must also deal with very large databases.
- *Privacy issues:* Forensic data is especially privacy-sensitive and it must be protected when outsourced. Actually, not only while outsourced, but it should be protected even when it is inside our own infrastructure to prevent non-authorized parties from accessing to the content.

In view of the above restrictions, several works have proposed solutions for the secure evaluation of PRNU-based camera attribution [3–5]: (1) In [3,4], Mohanty et al. combine the use of a trusted environment (ARM TrustZone) to compute the PRNU fingerprint, and the Boneh-Goh-Nissim (BGN) cryptosystem to perform the matching. (2) In [5], we proposed a more general formulation based on lattice cryptosystems. On the contrary to the previous method, our solution can be fully implemented on a general purpose arquitecture, and does not need to have access to a trusted environment because the involved images are encrypted along the whole computing chain.

Structure and Objectives: Our main objective in this work is to provide a brief overview of the existing secure schemes for PRNU-based camera attribution. With this in mind, we revisit the existing schemes and showcase how lattice-based cryptosystems are more convenient to perform the PRNU matching, improving the BGN-based solution in terms of efficiency, flexibility and privacy.

The structure is as follows: Section 2 describes the high-level structure of the two main existing secure approaches. Finally, Section 3 includes a discussion regarding the convenience of lattice-based cryptosystems for the case of PRNU matching, highlighting the flexibility of our solution.

2. Main Approaches

This section includes a high-level description of the two main methods for secure PRNU-based camera attribution: (a) Mohanty et al.'s scheme [3,4], and (b) our fully unattended solution from [5].

2.1. Previous Methods

In [3,4], Mohanty et al. describe their solution to securely compute the PRNU extraction/detection. It is composed of two main blocks:

- The Wavelet-based denoising is computed in a trusted environment (ARM TrustZone).
- The correlation test is homomorphically evaluated by means of the BGN cryptosystem.

The availability of a trusted environement enables to work very efficiently with the data in the clear. However, their use of the BGN cryptosystem introduces a high overhead (they report runtimes of 1.2 ms for the encryption of one number). To mitigate this effect, they resort to a fingerprint digest by removing some values of the fingerprint. This icreases the efficiency but also worsens the performance.

2.2. Our Fully Unattended Solution

In [5], we proposed a fully unattended solution, based on RLWE (Ring Learning with Errors) cryptosystems [6], which is able to homomorphically evaluate the PRNU extraction/detection without the need of the intervention of the secret key owner in the middle of the process. To this aim, we resort to the pre-/post processing introduced in [7] and the homomorphic Wavelet-denoising proposed in [8].

A complete diagram of our proposed scheme in [5] is included in Figure 1. The main challenge is the homomorphic evaluation of the threshold operation inside the denoising block. This threshold operation is implemented by the use of the "lowest digita removal" polynomials introduced in [9,10].

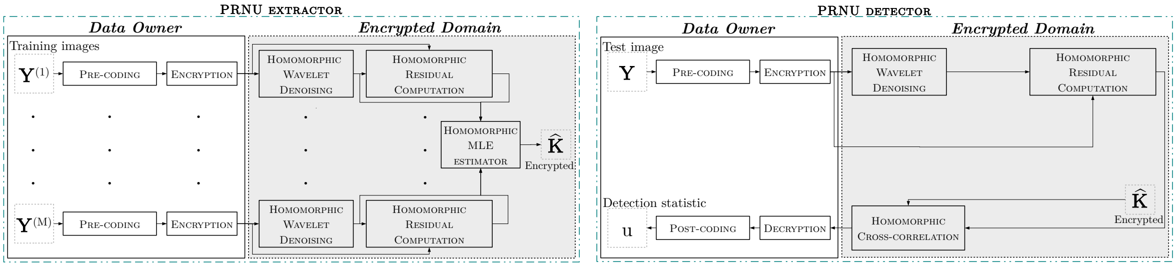

Figure 1. The secure PRNU extractor/detector proposed in [5].

We include some runtimes for the encrypted PRNU detection in Table 1. To obtain the given runtimes, images of size 2048 × 2048 and a PRNU of 16 Mpixels were considered.

The obtained results (see [5] for a much more detailed analysis) are promising as for all the conducted experiments, a True Acceptace Rate (TAR) of at least 95% was obtained for values of False Alarm Rate (FAR) above 0.5%.

Table 1. Performance of Encrypted PRNU detection (bit security > 128).

Parallelization	8	16
Encryption + Pre-coding (*s*)	3.6	
Decryption + Post-coding (*ms*)	27	
Encrypted Detection (*min*)	16.05	8.03

3. A Discussion: Efficient Encrypted Matching

This work reviews the existing methods in the literature for secure camera attribution based on PRNU. Even though the Mohanty et al.'s scheme is evaluating most of the computation in the clear, their runtimes do not outperform the runtimes obtained with our fully unattended proposed solution in [5]. This fact highlights the versatibility of our scheme, which can be implemented in a more general arquitecture and does not need a trusted environment. Even so, if a trusted environement is available, we could make use of it to have important efficiency improvements on the scheme.

It is worth noting that the BGN scheme seems to add a high overhead in the Mohanty et al.'s solution. By making use of an RLWE-based cryptosystem combined with a pre-/post-coding [11], the correlation runtimes are improved, while also avoiding to have to discard values of the fingerprint.

Funding: This research was funded by the Agencia Estatal de Investigación (Spain) and the European Regional Development Fund (ERDF) under projects WINTER (TEC2016-76409-C2-2-R) and COMONSENS (TEC2015-69648-REDC). Also funded by the Xunta de Galicia and the European Union (European Regional Development Fund - ERDF) under projects Agrupación Estratéxica Consolidada de Galicia accreditation 2016-2019 and Grupo de Referencia ED431C2017/53, and also by the FPI grant (BES-2014-069018).

Conflicts of Interest: The authors declare no conflict of interest. The funders had no role in the design of the study; in the collection, analyses, or interpretation of data; in the writing of the manuscript, or in the decision to publish the results.

References

1. Holst, G.C. *CCD Arrays, Cameras, and Displays*, 2nd ed.; SPIE Optical Engineering Press: Bellingham, WA, USA, 1998.
2. Chen, M.; Fridrich, J.; Goljan, M.; Lukáš, J. Determining Image Origin and Integrity Using Sensor Noise. *IEEE Trans. Inf. Forensics Secur.* **2008**, *3*, 74–90.
3. Mohanty, M.; Zhang, M.; Asghar, M.R.; Russello, G. PANDORA: Preserving Privacy in PRNU-Based Source Camera Attribution. In Proceedings of the 2018 17th IEEE International Conference on Trust, Security and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), New York, NY, USA, 1–3 August 2018; pp. 1202–1207.
4. Mohanty, M.; Zhang, M.; Asghar, M.R.; Russello, G. e-PRNU: Encrypted Domain PRNU-Based Camera Attribution for Preserving Privacy. *IEEE Trans. Dependable Secur. Comput.* **2019**, 1, doi:10.1109/TDSC.2019.2892448.
5. Pedrouzo-Ulloa, A.; Masciopinto, M.; Troncoso-Pastoriza, J.R.; Pérez-González, F. Camera Attribution Forensic Analyzer in the Encrypted Domain. In Proceedings of the 2018 IEEE International Workshop on Information Forensics and Security (WIFS), Hong Kong, China, 1–13 December 2018; pp. 1–7.
6. Lyubashevsky, V.; Peikert, C.; Regev, O. On Ideal Lattices and Learning with Errors over Rings. *J. ACM* **2013**, *60*, 43:1–43:35.
7. Pedrouzo-Ulloa, A.; Troncoso-Pastoriza, J.R.; Pérez-González, F. Number Theoretic Transforms for Secure Signal Processing. *IEEE Trans. Inf. Forensics Secur.* **2017**, *12*, 1125–1140.
8. Pedrouzo-Ulloa, A.; Troncoso-Pastoriza, J.R.; Pérez-González, F. Image Denoising in the Encrypted Domain. In Proceedings of the WIFS 2016: 8th IEEE International Workshop on Information Forensics and Security (WIFS), Abu Dhabi, UAE, 4–7 December 2016; pp. 1–6.
9. Griffin, M. Lowest Degree of Polynomial That Removes the First Digit of an Integer in Base. Available online: https://mathoverflow.net/q/269282 (accessed on 12 July 2019).

10. Chen, H.; Han, K. Homomorphic Lower Digits Removal and Improved FHE Bootstrapping. In Proceedings of the 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques (EUROCRYPT), Tel Aviv, Israel, 29 April–3 May 2018; pp. 315–337.
11. Pedrouzo-Ulloa, A.; Troncoso-Pastoriza, J.R.; Pérez-González, F. Revisiting Multivariate Lattices for Encrypted Signal Processing. In Proceedings of the 2018 ACM Conference on Economics and Computation, Ithaca, NY, USA, 18–22 June 2018; pp. 161–172.