EDITORES:

Manuel A. Serrano - Eduardo Fernández-Medina

Cristina Alcaraz - Noemí de Castro - Guillermo Calvo

Actas de las VI Jornadas Nacionales
(JNIC2021 LIVE)

INVESTIGACIÓN EN ciber segu ridad

Ediciones de la Universidad
de Castilla-La Mancha

Investigación en Ciberseguridad

Actas de las VI Jornadas Nacionales (JNIC2021 LIVE)

Online 9-10 de junio de 2021
Universidad de Castilla-La Mancha

Investigación en Ciberseguridad

Actas de las VI Jornadas Nacionales (JNIC2021 LIVE)

Online 9-10 de junio de 2021
Universidad de Castilla-La Mancha

Editores:
Manuel A. Serrano,
Eduardo Fernández-Medina,
Cristina Alcaraz
Noemí de Castro
Guillermo Calvo

Ediciones de la Universidad
de Castilla-La Mancha

Cuenca, 2021




Edita: Ediciones de la Universidad de Castilla-La Mancha

Colección JORNADAS Y CONGRESOS n.º 34

Esta editorial es miembro de la UNE, lo que garantiza la difusión y comercialización de sus publicaciones a nivel nacional e internacional.

I.S.B.N.: 978-84-9044-463-4
D.O.I.: http://doi.org/10.18239/jornadas_2021.34.00

Hecho en España (U.E.) – *Made in Spain (E.U.)*

Bienvenida del Comité Organizador

Tras la parada provocada por la pandemia en 2020, las VI Jornadas Nacionales de Investigación en Ciberseguridad (JNIC) vuelven el 9 y 10 de Junio del 2021 con energías renovadas, y por primera vez en su historia, en un formato 100% online. Esta edición de las JNIC es organizada por los grupos GSyA y Alarcos de la Universidad de Castilla-La Mancha en Ciudad Real, y con la activa colaboración del comité ejecutivo, de los presidentes de los distintos comités de programa y del Instituto Nacional de Ciberseguridad (INCIBE). Continúa de este modo la senda de consolidación de unas jornadas que se celebraron por primera vez en León en 2015 y le siguieron Granada, Madrid, San Sebastián y Cáceres, consecutivamente hasta 2019, y que, en condiciones normales se habrían celebrado en Ciudad Real en 2020.

Estas jornadas se han convertido en un foro de encuentro de los actores más relevantes en el ámbito de la ciberseguridad en España. En ellas, no sólo se presentan algunos de los trabajos científicos punteros en las diversas áreas de ciberseguridad, sino que se presta especial atención a la formación e innovación educativa en materia de ciberseguridad, y también a la conexión con la industria, a través de propuestas de transferencia de tecnología. Tanto es así que, este año se presentan en el Programa de Transferencia algunas modificaciones sobre su funcionamiento y desarrollo que han sido diseñadas con la intención de mejorarlo y hacerlo más valioso para toda la comunidad investigadora en ciberseguridad.

Además de lo anterior, en las JNIC estarán presentes excepcionales ponentes (Soledad Antelada, del Lawrence Berkeley National Laboratory, Ramsés Gallego, de Micro Focus y Mónica Mateos, del Mando Conjunto de Ciberdefensa) mediante tres charlas invitadas y se desarrollarán dos mesas redondas. Éstas contarán con la participación de las organizaciones más relevantes en el panorama industrial, social y de emprendimiento en relación con la ciberseguridad, analizando y debatiendo el papel que está tomando la ciberseguridad en distintos ámbitos relevantes.

En esta edición de JNIC se han establecido tres modalidades de contribuciones de investigación, los clásicos artículos largos de investigación original, los artículos cortos con investigación en un estado más preliminar, y resúmenes extendidos de publicaciones muy relevantes y de alto impacto en materia de ciberseguridad publicados entre los años 2019 y 2021. En el caso de contribuciones de formación e innovación educativa, y también de transferencias se han considerado solamente artículos largos. Se han recibido para su valoración un total de 86

contribuciones organizadas en 26, 27 y 33 artículos largos, cortos y resúmenes ya publicados, de los que los respectivos comités de programa han aceptado 21, 19 y 27, respectivamente. En total se ha contado con una ratio de aceptación del 77%. Estas cifras indican una participación en las jornadas que continúa creciendo, y una madurez del sector español de la ciberseguridad que ya cuenta con un volumen importante de publicaciones de alto impacto.

El formato online de esta edición de las jornadas nos ha motivado a organizar las jornadas de modo más compacto, distinguiendo por primera vez entre actividades plenarias (charlas invitadas, mesas redondas, sesión de formación e innovación educativa, sesión de transferencia de tecnología, junto a inauguración y clausura) y sesiones paralelas de presentación de artículos científicos. En concreto, se han organizado 10 sesiones de presentación de artículos científicos en dos líneas paralelas, sobre las siguientes temáticas: detección de intrusos y gestión de anomalías (I y II), ciberataques e inteligencia de amenazas, análisis forense y cibercrimen, ciberseguridad industrial, inteligencia artificial y ciberseguridad, gobierno y riesgo, tecnologías emergentes y entrenamiento, criptografía, y finalmente privacidad.

En esta edición de las jornadas se han organizado dos números especiales de revistas con elevado factor de impacto para que los artículos científicos mejor valorados por el comité de programa científico puedan enviar versiones extendidas de dichos artículos. Adicionalmente, se han otorgado premios al mejor artículo en cada una de las categorías. En el marco de las JNIC también hemos contado con la participación de la Red de Excelencia Nacional de Investigación en Ciberseguridad (RENIC), impulsando la ciberseguridad a través de la entrega de los premios al *Mejor Trabajo Fin de Máster en Ciberseguridad* y a la *Mejor Tesis Doctoral en Ciberseguridad*. También se ha querido acercar a los jóvenes talentos en ciberseguridad a las JNIC, a través de un CTF (Capture The Flag) organizado por la Universidad de Extremadura y patrocinado por Viewnext.

Desde el equipo que hemos organizado las JNIC2021 queremos agradecer a todas aquellas personas y entidades que han hecho posible su celebración, comenzando por los autores de los distintos trabajos enviados y los asistentes a las jornadas, los tres ponentes invitados, las personas y organizaciones que han participado en las dos mesas redondas, los integrantes de los distintos comités de programa por sus interesantes comentarios en los procesos de revisión y por su colaboración durante las fases de discusión y debate interno, los presidentes de las sesiones, la Universidad de Extremadura por organizar el CTF y la empresa Viewnext por patrocinarlo, los técnicos del área TIC de la UCLM por el apoyo con la plataforma de comunicación, los voluntarios de la UCLM y al resto de organizaciones y entidades patrocinadoras, entre las que se encuentra la Escuela Superior de Informática, el Departamento de Tecnologías y Sistemas de Información y el Instituto de Tecnologías y Sistemas de Información, todos ellos de la Universidad de Castilla-La Mancha, la red RENIC, las cátedras (Telefónica e Indra) y aulas (Avanttic y Alpinia) de la Escuela Superior de Informática, la empresa Cojali, y muy especialmente por su apoyo y contribución al propio INCIBE.

Manuel A. Serrano, Eduardo Fernández-Medina
Presidentes del Comité Organizador
Cristina Alcaraz
Presidenta del Comité de Programa Científico
Noemí de Castro
Presidenta del Comité de Programa de Formación e Innovación Educativa
Guillermo Calvo Flores
Presidente del Comité de Transferencia Tecnológica

Índice General

Comité Ejecutivo

Juan Díez González	INCIBE
Luis Javier García Villalba	Universidad de Complutense de Madrid
Eduardo Fernández-Medina Patón	Universidad de Castilla-La Mancha
Guillermo Suárez-Tangil	IMDEA Networks Institute
Andrés Caro Lindo	Universidad de Extremadura
Pedro García Teodoro	Universidad de Granada. Representante de red RENIC
Noemí de Castro García	Universidad de León
Rafael María Estepa Alonso	Universidad de Sevilla
Pedro Peris López	Universidad Carlos III de Madrid

Comité Organizador

Presidentes del Comité Organizador

Eduardo Fernández-Medina Patón	Universidad de Castilla-la Mancha
Manuel Ángel Serrano Martín	Universidad de Castilla-la Mancha

Finanzas

David García Rosado	Universidad de Castilla-la Mancha
Luis Enrique Sánchez Crespo	Universidad de Castilla-la Mancha

Actas

Antonio Santos-Olmo Parra	Universidad de Castilla-la Mancha

Difusión

Julio Moreno García-Nieto	Universidad de Castilla-la Mancha
José Antonio Cruz Lemus	Universidad de Castilla-la Mancha
María A Moraga de la Rubia	Universidad de Castilla-la Mancha

Webmaster

Aurelio José Horneros Cano	Universidad de Castilla-la Mancha

Logística y Organización

Ignacio García-Rodriguez de Guzmán	Universidad de Castilla-la Mancha
Ismael Caballero Muñoz-Reja	Universidad de Castilla-la Mancha
Gregoria Romero Grande	Universidad de Castilla-la Mancha
Natalia Sanchez Pinilla	Universidad de Castilla-la Mancha

Comité de Programa Científico

Presidenta

Cristina Alcaraz Tello	Universidad de Málaga

Miembros

Aitana Alonso Nogueira	INCIBE
Marcos Arjona Fernández	ElevenPaths
Ana Ayerbe Fernández-Cuesta	Tecnalia
Marta Beltrán Pardo	Universidad Rey Juan Carlos
Carlos Blanco Bueno	Universidad de Cantabria
Jorge Blasco Alís	Royal Holloway, University of London
Pino Caballero-Gil	Universidad de La Laguna
Andrés Caro Lindo	Universidad de Extremadura
Jordi Castellà Roca	Universitat Rovira i Virgili
José M. de Fuentes García-Romero de Tejada	Universidad Carlos III de Madrid
Jesús Esteban Díaz Verdejo	Universidad de Granada
Josep Lluis Ferrer Gomila	Universitat de les Illes Balears
Dario Fiore	IMDEA Software Institute
David García Rosado	Universidad de Castilla-La Mancha
Pedro García Teodoro	Universidad de Granada
Luis Javier García Villalba	Universidad Complutense de Madrid
Iñaki Garitano Garitano	Mondragon Unibertsitatea
Félix Gómez Mármol	Universidad de Murcia
Lorena González Manzano	Universidad Carlos III de Madrid
María Isabel González Vasco	Universidad Rey Juan Carlos I
Julio César Hernández Castro	University of Kent
Luis Hernández Encinas	CSIC
Jorge López Hernández-Ardieta	Banco Santander
Javier López Muñoz	Universidad de Málaga
Rafael Martínez Gasca	Universidad de Sevilla
Gregorio Martínez Pérez	Universidad de Murcia

David Megías Jiménez	Universitat Oberta de Cataluña
Luis Panizo Alonso	Universidad de León
Fernando Pérez González	Universidad de Vigo
Aljosa Pasic	ATOS
Ricardo J. Rodríguez	Universidad de Zaragoza
Fernando Román Muñoz	Universidad Complutense de Madrid
Luis Enrique Sánchez Crespo	Universidad de Castilla-La Mancha
José Soler	Technical University of Denmark-DTU
Miguel Soriano Ibáñez	Universidad Politécnica de Cataluña
Victor A. Villagrá González	Universidad Politécnica de Madrid
Urko Zurutuza Ortega	Mondragon Unibertsitatea
Lilian Adkinson Orellana	Gradiant
Juan Hernández Serrano	Universitat Politécnica de Cataluña

Comité de Programa de Formación e Innovación Educativa

Presidenta

Noemí De Castro García	Universidad de León

Miembros

Adriana Suárez Corona	Universidad de León
Raquel Poy Castro	Universidad de León
José Carlos Sancho Núñez	Universidad de Extremadura
Isaac Agudo Ruiz	Universidad de Málaga
Ana Isabel González-Tablas Ferreres	Universidad Carlos III de Madrid
Xavier Larriva	Universidad Politécnica de Madrid
Ana Lucila Sandoval Orozco	Universidad Complutense de Madrid
Lorena González Manzano	Universidad Carlos III de Madrid
María Isabel González Vasco	Universidad Rey Juan Carlos
David García Rosado	Universidad de Castilla - La Mancha
Sara García Bécares	INCIBE

Comité de Transferencia Tecnológica

Presidente

Guillermo Calvo Flores	INCIBE

Miembros

José Luis González Sánchez	COMPUTAEX
Marcos Arjona Fernández	ElevenPaths
Victor Villagrá González	Universidad Politécnica de Madrid
Luis Enrique Sánchez Crespo	Universidad de Castilla – La Mancha

Sesión de Investigación A4: Análisis forense y cibercrimen
http://doi.org/10.18239/jornadas_2021.34.23

A Review of "Camera Attribution Forensic Analyzer in the Encrypted Domain"

A. Pedrouzo-Ulloa
atlanTTic, UVigo, Spain
apedrouzo@gts.uvigo.es

M. Masciopinto
atlanTTic, UVigo, Spain
mmasciopinto@gts.uvigo.es

J. R. Troncoso-Pastoriza
EPFL, Switzerland
juan.troncoso-pastoriza@epfl.ch

F. Pérez-González
atlanTTic, UVigo, Spain
fperez@gts.uvigo.es

***Abstract*—This paper is a review of a work previously published by the authors at IEEE WIFS'18 (Workshop on Information Forensics and Security), which received the Best Paper Award, and contains a summary of its main results. In WIFS'18 we proposed a new framework for the secure outsourcing of the image source attribution problem, in which the Photoresponse Non-Uniformity (PRNU) is used as a fingerprint to decide whether a test image was taken with a specific camera device. This method is fully unattended, that is, the secret key owner does not take part during the process. To this aim, we introduced improvements on the state-of-the-art in secure and unattended solutions for denoising. We also showed how to homomorphically perform filtering, polynomial, denoising and pixel-wise operations in a single round without the need of an interactive protocol.**

***Index Terms*—Photoresponse Non-Uniformity; lattice-based cryptosystems; digital media forensics; camera attribution forensic analyzer**

Type of contribution: *Already published research*

I. Introduction

In this paper we present the results of our research that was previously published at the Workshop on Information Forensics and Security (WIFS) in 2018 [1].

A. Motivation

All digital imaging sensors intrinsically present a noise pattern called PRNU, which is due to tiny and random imperfections on the silicon wafer. PRNU is becoming particularly relevant within digital media forensics, as it can be used as a fingerprint to determine whether a given image was taken by a certain device. Consequently, many works have made use of its uniqueness feature for a wide range of applications; which includes identification and clustering of acquisition devices.

However, an important problem that these applications share is that they are computationally intensive and work with very large databases. Actually, although buying computing power and database storage as needed appears as an interesting solution, the privacy-sensitive nature of forensic data prevents from directly outsourcing it unencrypted.

Recent results from [2], [3] show that the estimated PRNU fingerprints leak a considerable amount of information of the images used for extraction. This constitutes a serious privacy threat and suggests that for some scenarios (e.g., child pornography crimes), camera fingerprints should be protected not only when outsourcing, but at all times during investigations.

B. Main results of [1]

The secure scheme proposed in [1] was exemplified for the case of PRNU extraction/detection, but it covers many other forensic tools.

The main technical results are the following:

- An efficient Wavelet-based denoising primitive is introduced. The main novelty relies on the use of a new homomorphic threshold function by means of the "lowest digit removal" polynomials introduced in [4], [5].
- Further optimizations on the Wavelet denoising primitive are presented, consisting of the use of efficient NTT (Number Theoretic Transforms) packing.
- The previous encrypted denoising primitive is used as a building block in a more complex use case as the PRNU extraction/detection for camera attribution. The proposed method is able to compute the process for extraction/detection in an unattended way, that is, without additional interactions between the client and server.

II. Proposed Scheme

A. Related Works

To the best of our knowledge [6], there are two different approaches for secure camera attribution: (a) Mohanty *et al.,* [7], [8] who combine a trusted environment (ARM TrustZone) for the computation of the PRNU fingerprint, with the Boneh-Goh-Nissim (BGN) cryptosystem for the matching, and (b) ours [1], which proposes a more flexible solution that can be implemented on a general purpose architecture and does not require access to a trusted environment.

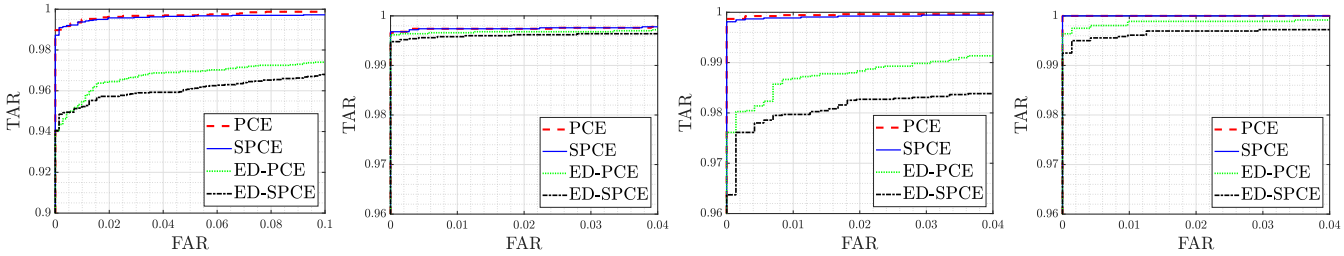
As we discussed in [6], although Mohanty *et al.*'s scheme evaluates most of the computation in the clear, their runtimes do not improve those obtained by our solution. In fact, the PRNU matching in their scheme could be more efficiently calculated by substituting the BGN cryptosystem with more modern lattice-based cryptosystems. In relation to this, it is worth mentioning that, if available, our solution could also use a trusted environment to improve the efficiency.

B. Unattended and Secure Camera Attribution

Our proposed scheme is based on the use of an RLWE (Ring Learning with Errors) cryptosystem equipped with an adequate use of NTT transforms and efficient signal pre-/post-coding operations before/after encryption/decryption.

Due to space restrictions, we refer the reader to [1] for more details. A full diagram of the proposed framework is included in [1, Fig. 1].

The main challenge is the efficient evaluation of the threshold function used in the Wavelet denoising primitive. By approximating this threshold with a quantization operation, we can leverage the "lowest digit removal" polynomials as a mechanism to homomorphically evaluate thresholding. The



(a) Nikon D7000. (b) Nikon D90. (c) Canon 1100D. (d) Nikon D3000.

Fig. 1: True Acceptance Rate (TAR) vs. False Alarm Rate (FAR) for 4 different camera devices. PCE represents the result obtained with the denoising in [9] and the PCE statistic [10], SPCE is the simplified detector in [1, eq. (4)] applying the denoising from [9], ED-PCE is the PCE statistic using the encrypted denoising described in [1, Sec. 3.2], and ED-SPCE stands for the simplified detector discussed in [1, Sec. 3].

use of this functionality results in a considerably reduction of the ciphertext size and the depth of circuit to be computed.

III. Performance Evaluation

We evaluated in [1] our secure framework in terms of efficiency, security and performance. To this aim, we securely performed the PRNU detection test, in which the PRNU estimate is tested against the test image via the statistical distribution of a score on both hypothesis (i.e., the image contains or not the PRNU estimate); whereas the PRNU estimate was obtained in the clear domain.

This scenario corresponds to the case where the police have confiscated the camera of a suspect, and would like to check whether an image has been taken by this camera.

Due to legal restrictions, this test image cannot be outsourced without being previously protected. On the contrary, as we have control of the camera, we can take flatfield images to perform the extraction without any privacy leakage.

A. Implementation and execution times

We implemented our scheme taking advantage of the RNS variant of the FV cryptosystem [1], and execution times were measured on an Intel Xeon E5-2667V3 at 3.2GHz using one core for the non-parallelized choice.

Table I reports the runtimes for encrypted detection assuming that the PRNU estimate and the test image are aligned.

TABLE I: Runtimes for Encrypted PRNU detection (2048×2048 image)

Parallelization (cores)	1	8	16	20
Encrypted Detection (min)	128.33	16.05	8.03	6.53
Encryption + Pre-coding (s)	3.6 (1 core, client-side)			
Decryption + Post-coding (ms)	27 (1 core, client-side)			

The introduced improvements on the unattended denoising primitive result to be fundamental in achieving the above execution runtimes.

B. PRNU Detection Performance

We utilized a database composed of 2639 TIFF images taken from 16 digital camera devices. The fingerprint was extracted for each different camera device from 50 randomly chosen TIFF images. For the detection phase, we considered crops of the JPEG-compressed version of the TIFF images with size 1536×1536 and a quality factor of 95.

Figure 1 compares the performance of the detector in [1, Eq. (2)] (dot product) with the Peak to Correlation Energy (PCE) detector [10], both when the popularly used image denoising in [9] and when our encrypted denoising are used to obtain the residues of the different test images. As the fingerprint estimate is obtained in the clear, we used in all the experiments the denoising method from [9] for extraction.

IV. Conclusions and Future Work

This work reviews the results obtained in a previously published paper [1] by the authors. In [1], we introduced an unattended secure framework for outsourcing computation which could perform the PRNU extraction/detection phases without any additional interaction with the client. We evaluated the performance of our method in a concrete scenario on which the test images have to be protected.

Our results show the feasibility of source camera attribution in the encrypted domain. Even so, there is still room for improvement, and we are currently working on a complete evaluation of the encrypted extraction. This includes further refinements on the encrypted denoising primitive, and a reevaluation of the use of the underlying RLWE cryptosystem profiting from the most recent results in the field.

Acknowledgments

GPSC is funded by the Agencia Estatal de Investigación (Spain) and the European Regional Development Fund (ERDF) under project RODIN (PID2019-105717RB-C21). Also funded by the Xunta de Galicia and the European Union (European Regional Development Fund - ERDF) under projects ED431G2019/08 and Grupo de Referencia ED431C2017/53.

References

[1] A. Pedrouzo-Ulloa, M. Masciopinto, J. R. Troncoso-Pastoriza, and F. Pérez-González, "Camera Attribution Forensic Analyzer in the Encrypted Domain," in *IEEE WIFS*, 2018, pp. 1–7.

[2] S. Fernández-Menduiña and F. Pérez-González, "On the Information Leakage of Camera Fingerprint Estimates," 2020.

[3] F. Pérez-González and S. Fernández-Menduiña, "Prnu-leaks: facts and remedies," in *EUSIPCO 2020*. IEEE, 2020, pp. 720–724.

[4] M. Griffin, "Lowest degree of polynomial that removes the first digit of an integer in base p," https://mathoverflow.net/q/269282, accessed: 10 March 2020.

[5] H. Chen and K. Han, "Homomorphic Lower Digits Removal and Improved FHE Bootstrapping," in *EUROCRYPT*, 2018, pp. 315–337.

[6] A. Pedrouzo-Ulloa, M. Masciopinto, J. R. Troncoso-Pastoriza, and F. Pérez-González, "Efficient PRNU Matching in the Encrypted Domain," in *XoveTIC*. MDPI, 2019.

[7] M. Mohanty, M. Zhang, M. R. Asghar, and G. Russello, "PANDORA: Preserving Privacy in PRNU-Based Source Camera Attribution," in *IEEE TrustCom/BigDataSE*, 2018, pp. 1202–1207.

[8] M. Mohanty, M. Zhang, M. R. Asghar, and G. Russello, "e-PRNU: Encrypted Domain PRNU-Based Camera Attribution for Preserving Privacy," *IEEE Trans. Dependable and Sec. Computing*, pp. 1–1, 2019.

[9] M. K. Mihcak, I. Kozintsev, and K. Ramchandran, "Spatially adaptive statistical modeling of wavelet image coefficients and its application to denoising," in *IEEE ICASSP*, vol. 6, 1999, pp. 3253–3256.

[10] M. Goljan, J. Fridrich, and T. Filler, "Large scale test of sensor fingerprint camera identification," in *Proc. SPIE, Electronic Imaging, Media Forensics and Security XI*, vol. 7254, Feb. 2009, pp. 0I 1-0I 12.