Leveraging image noise: source camera identification and increased robustness of convolutional neural networks

Bennabhaktula, Guru Swaroop

DOI:
10.33612/diss.843513794

Leveraging image noise:
Source camera identification and increased robustness of convolutional neural networks

Guru Swaroop Bennabhaktula

This research has been conducted at the Information Systems group of the Bernoulli Institute for Mathematics, Computer Science and Artificial Intelligence of the University of Groningen, and at the Group for Vision and Intelligent Systems at the Department of Electrical, Systems, and Automation of the University of León.

This work was partly supported by the framework agreement between the University of León and INCIBE (Spanish National Cybersecurity Institute) under Addendum 01. This research has been partly funded with support from the European Commission under the 4NSEEK project with Grant Agreement 821966.

Cover image: The picturesque landscape is from Alt St. Johann in Switzerland, taken during the memorable SSSIHL alumni retreat (SEAM 2022). It illustrates, on the left, the manifestation of the hidden camera noise used in forensic analysis. On the right is a representation of the high-level scene content in images useful in the design of robust computer vision models.

AIO

Cover design: Proefschrift AIO | Guntra Laivacuma
Printed by: Proefschrift AIO

university of groningen

universidad de león

Leveraging image noise: source camera identification and increased robustness of convolutional neural networks

PhD thesis

to obtain the degree of PhD of the
University of Groningen
on the authority of the
Rector Magnificus Prof. J.M.A. Scherpen
and in accordance with
the decision by the College of Deans

and

to obtain the degree of PhD of the
University of León
on the authority of the
Rector Magnificus Prof. J.F.G. Marín
and in accordance with
the decision by the College of Deans.

Double PhD degree

This thesis will be defended in public on

Monday 18 December 2023 at 14.30 hours

by

Guru Swaroop Bennabhaktula

born on 13 August 1991
in Visakhapatnam, India

Supervisors

Prof. D. Karastoyanova
Prof. E. Alegre

Co-supervisor

Dr. G. Azzopardi

Assessment Committee

Prof. M. Castejon Limas
Prof. M. Biehl
Prof. A. Telea
Prof. D. Meuwly

Dedicated with Love to
Bhagawan Sri Sathya Sai Baba

Contents

Tabla de contenido en español

Acknowledgements

The journey leading to the preparation of this thesis has been both challenging and fun. It goes without saying this was made possible only by the support and guidance of family, friends, colleagues, well-wishers, and most importantly my beloved God. I am immensely grateful to everyone.

Firstly, I would like to express my gratitude to my mother and father for always supporting me and playing a vital role in my upbringing. In spite of being far away in India, my father was always available to have a conversation with me whenever I reached out to him. I look up to him for his qualities of forbearance, hard work, sincerity, and love. These helped me cultivate a part of my personality that helped me immensely during my PhD studies and beyond.

Teachers are the pillars of this society. I consider myself very fortunate to have been guided by selfless teachers who inculcated noble values along with secular education. Particularly, I am grateful to all the teachers from the Sri Sathya Sai Educational Institutions in India, with whom I had the opportunity to interact and learn. I am indebted to all of them. I would especially like to thank Prof. Raghunatha Sarma and Prof. Pallav Kumar Baruah for their support in guiding and inspiring me to pursue a Ph.D. degree. I am also grateful to the supervisors of my Master's thesis Dr. Srikanth Khanna and Prof. Venkatachalam Chandrasekaran who have been instrumental in helping me develop personal and research skills necessary for my career.

Coming to the Ph.D. thesis itself, the most important people behind its success are, of course, my supervisors. I had the opportunity to be supervised by Prof. Dimka Karastoyanova and Dr. George Azzopardi from the University of Groningen, the Netherlands, and Prof. Enrique Alegre from the University of Léon, Spain. It was a valuable learning experience for me both professionally and personally. George played the role of a daily supervisor and his involvement and interest in the project was beyond my expectation. We had a lot of interesting interactions on several ideas related to our project and sometimes these were

virtually late in the evenings while working from home. I am sure this wouldn't have happened without the understanding of George's wife Charmaine, and their daughters Alaia and Amira. I thank you all for your support. I would like to express my deepest sense of gratitude to all my supervisors for the opportunities they have provided me for my growth.

My stay at Groningen was pleasant due to my colleagues from the Information Systems Group and Artificial Intelligence group. I would like to thank Abolfazl, Ali Reza, Mohammed Alghazwi, Arash, Xueyi, Nafiseh, Estefania, Ahmad, Sreejita, and Anusha. Likewise, I would like to thank my colleagues from the GVIS research group in Léon. I must mention that it is because of you that my stay in Léon became possible and comfortable due to your assistance with Spanish and local arrangements. I would like to thank Surajit, Eduardo, Victor, Laura, Rubel, David, Pablo, Aitor, Andres, Fran, Javier, and Manuel. I also cherish the collaborations with students in their Master's and Bachelor studies. Thanks to Derrick, Joey, Adrain, and Thijs. I would also like to thank Peter van der wal for reviewing the Dutch versions of my thesis.

Family and friends are very important to your well-being. I was lucky enough to have the company of my cousin Pushpa in Groningen. Along with Sukhmander, we all enjoyed preparing nice dinners, praying, and having a good time together. Incidentally, I was also lucky to have the company of my cousin Vishal in Léon. Thanks to Ali Reza and Pushpa for kindly agreeing to be my paranymphs. Although the rest of my family was in India, they were in constant touch and never let me feel that I was physically far away. I thank you all for your love and care.

I would fail in my duty if I did not thank all the administrative and support staff at both the Universities of Groningen and Léon. They did a phenomenal job in taking care of several things right from the issue of contracts, arranging residence permits, and finally getting the double doctorate agreement signed. I would like to especially thank the HPC group at Groningen for providing access to the Peregrine supercomputer and the team at Léon for similar access to computing resources.

Finally, I would like to express my deepest sense of gratitude to Bhagawan Sri Sathya Sai Baba. I remember His words, rephrased, "A Ph.D. is of no use to the nation if it cannot be applied for the welfare of the society". I am grateful to Him for providing me with a topic that has a societal impact. I know that I am merely an instrument and He is the real doer. I am ever grateful for His guidance and for giving me this experience.

Guru Swaroop Bennabhaktula
Groningen
November 22, 2023

List of Figures

List of Tables

List of acronyms

4NSEEK Forensic Against Sexual Exploitation of Children

AWGN Additive White Gaussian Noise

BN Batch Normalization

CCD Charge Coupled Device

CFA Color Filter Array

CNN Convolutional Neural Network

Conv Convolutional

ConvNet Convolutional Neural Network

CORF Combination of Receptive Fields

EXIF Exchangeable Image File

FC Fully Connected

FPN Fixed Pattern Noise

FN False Negatives

FP False Positives

LEA Law Enforcement Agency

MaxPool Max-Pooling

MISLNet ConvNet architecture proposed by Bayar and Stamm (2018a)

PNU Pixel Non-Uniformity noise

PRNU Photo Response Non-Uniform noise

QUFVD Qatar University Forensic Video Database

ReLU Rectified Linear Unit

RGB Red, Green, and Blue image-colour channels

SCI Source Camera Identification

SGD Stochastic Gradient Descent

SPN Sensor Pattern Noise

SVM Support Vector Machine

TP True Positives

Spanish abstract

El ruido en una imagen digital puede ser una ventaja o una desventaja dependiendo del problema con el que se esté trabajando. Analizando el ruido de la imagen, esta tesis estudia y propone soluciones a dos aplicaciones diferentes del mismo. En la primera, se explora el papel del ruido generado por los sensores de una cámara para realizar un análisis forense de medios digitales donde la presencia de ruido en una imagen resulta crucial. Este trabajo se realizó dentro del proyecto 4NSEEK (análisis forense contra el abuso sexual de menores), financiado por la UE, que aborda un importante problema social. La otra línea en la que se trabaja en esta tesis es la vulnerabilidad de los sistemas de aprendizaje profundo frente al ruido presente en la imagen de entrada, para lo que se proponen medidas para mitigar el impacto de dicho ruido.

La primera parte de la tesis aborda varias cuestiones de investigación centradas en identficar la cámara con la que se ha obtenido una imagen o un vídeo. En primer lugar, dado un par de imágenes, se pretende determinar la probabilidad de que ambas hayan sido capturadas utilizando la misma cámara Para ello, se propone una red que consta de dos partes: la primera extrae huellas forenses de cada imagen y la segunda coteja un par de dichas huellas para establecer la similitud con otra imagen determinando así la cámara con la que se obtuvo. Hasta donde tenemos constancia, esta es la primera propuesta que aborda el problema de identificar qué dispositivo obtuvo una imagen determinada, mostrandose con los resultados obtenidos el potencial de esta línea de investigación. En segundo lugar, se pretende conocer si algunas regiones de una imagen tienen una mayor presencia de ruido de cámara que otras. Para responder a esta pregunta, se examinaron diferentes regiones de una imagen y se planteó la hipótesis de que las regiones homogéneas de una imagen son las menos distorsionadas en comparación con las regiones con detalles de alto nivel de la escena, como bordes y patrones de textura.

Posteriormente, propusimos un sistema jerárquico para identficar las cámaras basado en parches homogéneos. La metodología propuesta alcanzó una precisión de clasificación del 99,01% en el conjunto de datos públicos de Dresde para la identificación de modelos de cámara. Además, el esquema de clasificación jerárquica propuesto hace que el sistema sea modular y facilita que se amplíe eficientemente con la incorporación de nuevos dispositivos de cámara. Nos basamos en el trabajo de Bayar and Stamm (2018a) que propuso una convolución restringida de un solo canal para suprimir el contenido de la escena, ampliando la solución propuesta en este trabajo a una solución multicanal. El tercer problema que propusimos resolver fue determinar en qué configuraciones de redes neuronales convolucionales (ConNets) son eficaces las convoluciones restringidas. Se comprobó empíricamente que las convoluciones restringidas sólo son eficaces con ConvNets poco profundas y no con ConvNets profundas. Además, en el análisis forense de vídeos, se examinó qué fotogramas de vídeo conservaban más rastros forenses. Se abordó el problema consistente en extraer rastros forenses de vídeos comprimidos como los de YouTube y WhatsApp para observar que los fotogramas I retienen mejores rastros forenses en comparación con los demás. Posteriormente, se observó que, incluso con las compresiones de WhatsApp y YouTube, el sistema es capaz de identificar la cámara de origen con la misma precisión que en los vídeos nativos.

La segunda parte de la tesis se centra en hacer que los sistemas de aprendizaje profundo sean robustos frente a la corrupción de imágenes no vistas previamente. Alejándose del enfoque tradicional, que consiste en utilizar la aumentación de datos para mejorar la robustez, el objetivo que se tuvo fue explorar métodos alternativos para lograr la generalización fuera de la distribución original. En el primer enfoque, se propone un nuevo paso de preprocesamiento de datos, en el que se utilizan mapas de delineación CORF en lugar de la imagen tradicional como entrada a la ConvNet. Esto mejoró significativamente la robustez del modelo frente al ruido aleatorio uniforme y gaussiano, con una precisión comparable a la obtenida en imágenes de prueba limpias. Posteriormente, se propone una novedosa modificación intrínseca de la arquitectura de ConvNet para hacerla robusta frente a distintos tipos de corrupción de imágenes. En concreto, se propone una convolución basada en push-pull para sustituir la primera capa convolucional de una ConvNet. Los amplios experimentos realizados con los conjuntos de datos ImageNet-C y CIFAR10-C demuestran la eficacia de este enfoque.