Federica Granese

+39 (328) 5611357 federica.granese@ird.fr https://fgranese.github.io/ https://github.com/fgranese

PhD graduate with a comprehensive background in Computer Science (Bachelor's, Master's, and PhD), my interests are centered on the intersection of security in machine learning and the application of machine learning in the medical field. I am a highly motivated worker, skilled in object-oriented programming, and well-versed in the information-theoretical aspects of machine learning.

Spoken Languages: Italian (native), English (fluent), French (intermediate), Spanish (beginner).

Education

PhD in Computer Science **April 2023**
Towards Securing Machine Learning Algorithms through Misclassification Detection and Adversarial Attack Detection
École Polytechnique, Paris, France
Joint PhD with Sapienza University, Roma, Italy

M.S. in Computer Science **October 2019**
Enhanced models for privacy and utility in continuous-time diffusion networks *110/110 cum laude*
Sapienza University, Roma, Italy

B.S. in Computer Science **October 2017**
Polynomially Recognising Graphs Where Saturating Flows are Always Maximum *106/110*
Sapienza University, Roma, Italy

Experience

Postdoctoral Fellow **April 2023 - Present**
DeepECG4U - artificial intelligence in the service of heart health
Sorbonne Université, Paris, France
Institut de Recherche pour le Développement (IRD) UMMISCO, Bondy, France

- Enhance the robustness of Electrocardiogram classifiers specifically for arrhythmia prediction.
- Study the impact of Electrocardiogram denoising on automated classification and its consequential implications on the reliability of the models.
- Investigate generative models for Electrocardiogram reconstruction.

Research Internship **October 2022 - March 2023**
How to detect errors in image segmentation tasks
École de technologie supérieure (ÉTS), Montreal, Canada

- Conducted research on advanced models for segmenting tumors in MRI images.
- Investigated model calibration techniques and their impact on the misclassification detection task.

PhD Candidate **October 2019 - April 2023**
Safety and Security in AI
Inria-Saclay, Paris, France

- Contributed to new research topics on misclassification detection, i.e., the problem of identifying whether the prediction of a DNN classifier should (or should not) be trusted.
- Contributed to new research topics on multi-armed adversarial attacks detection, i.e., the problem of identifying simultaneous adversarial attacks perpetrated over the DNN classifier.
- Conducted research on estimating the privacy level of various notions of differential privacy.
- Designed, developed, and maintained code repository to support result reproducibility.

Research Internship **March 2019 - July 2019**
Diffusion of information in social networks
Inria-Saclay, Paris, France

- Conducted research on modeling the diffusion of information in social networks to meet privacy and utility guarantees.
- Contributed to a new formulation of utility/privacy policies, aiming to maximize the delivery of information to intended users while minimizing its reach to unintended ones.

Research Internship **March 2017 - September 2017**

Algorithm design network flows

Sapienza University, Rome, Italy

- Conducted research on network models where information items flow from a source vertex to a sink vertex, specifically standard flow networks with capacity on edges.
- Contributed to a new polynomial-time algorithm for ensuring that every saturating flow under every capacity-to-edge assignment is maximum.

TEACHING

- Mécanismes de la programmation orientée-objet, *Object-oriented programming mechanics*. TA (Java). École Polytechnique, Academic Year 2019-2020.
- Mécanismes de la programmation orientée-objet, *Object-oriented programming mechanics*. TA (Java). École Polytechnique, Academic Year 2020-2021.

PROGRAMMING SKILLS

Programming Languages: C, Python, Java, Bash, SQL, HTML.
Frameworks and Libraries: PyTorch, TensorFlow, SciKit.
Deployment: Git, Jupyter Notebooks.
Document Preparation Systems: LATEX, Markdown.
DBMSs MySQL, PostgreSQL.
Operative Systems: MacOS, Linux (Ubuntu Desktop), Windows.

AWARDS AND SCHOLARSHIPS

- Bourse de recherche Mitacs Globalink (2022), 6 months mobility. (**6.000 CAD**).
- Vinci, Chapter II (2020). Competition for financing thesis in cotutelle between Italy and France (**4.700 Eur**).
- Erasmus+ (AY 2018 – 2019), 6 months mobility. (**1.000 Eur**).
- ACM Celebration of Women in Computing (womENcourage2019), AI and Welfare. 16-18 September (2019).

PUBLICATIONS

Proceedings of International Conferences and Journal Papers

Optimal Zero-Shot Detector for Multi-Armed Attacks.
Federica Granese, Marco Romanelli, Pablo Piantanida.
AISTATS 2024 (to appear).

On the (Im)Possibility of Estimating Various Notions of Differential Privacy (short paper).
Daniele Gorla, Louis Jalouzot, Federica Granese, Catuscia Palamidessi, Pablo Piantanida.
ICTCS 2023: 219-224.

A Halfspace-Mass Depth-Based Method for Adversarial Attack Detection.
Marine Picot, Federica Granese, Guillaume Staerman, Marco Romanelli, Francisco Messina, Pablo Piantanida, Pierre Colombo.
Transaction on Machine Learning Research (2023).

MEAD: A Multi-Armed Approach for Evaluation of Adversarial Examples Detectors.
Federica Granese, Marine Picot, Marco Romanelli, Francisco Messina, Pablo Piantanida.
ECML/PKDD (3) 2022: 286-303.

Enhanced models for privacy and utility in continuous-time diffusion networks.
Federica Granese, Daniele Gorla, Catuscia Palamidessi.
Int. J. Inf. Sec. 20(5): 763-782 (2021).

DOCTOR: A Simple Method for Detecting Misclassification Errors.
Federica Granese, Marco Romanelli, Daniele Gorla, Catuscia Palamidessi, Pablo Piantanida.
NeurIPS 2021: 5669-5681. Spotlight.

Enhanced Models for Privacy and Utility in Continuous-Time Diffusion Networks.
Daniele Gorla, Federica Granese, Catuscia Palamidessi.
ICTAC 2019: 313-331.

Preprints

A simple Training-Free Method for Rejection Option.
Eduardo Dadalto Câmara Gomes, Marco Romanelli, Federica Granese, Pablo Piantanida.
Paper under review.

On the (Im)Possibility of Estimating Various Notions of Differential Privacy.
Daniele Gorla, Louis Jalouzot, Federica Granese, Catuscia Palamidessi, Pablo Piantanida.
CoRR abs/2208.14414 (2022)

Workshops

The Negative Impact of Denoising on Automated Classification of Electrocardiograms.
Federica Granese, Ahmad Fall, Alex Lence, Joe-Elie Salem, Jean-Daniel Zucker, Edi Prifti.
Deep Generative Models for Health Workshop NeurIPS 2023.

ORAL COMMUNICATIONS

- Séminaire COMCYBER/IA. ≪ Fiabilité, confiance, éthique : quelle sécurité des IA ? ≫. 31 Jennuary 2024, Maison des Polytechniciens, Paris.
- Génération IA 2030. Colloque européen sur l'Intelligence Artificielle. 14-18 March 2022, DigitalCity. Bruxelles.
- DATAIA Workshop ≪ Safety & AI ≫ 2021. 13 December 2021, Centre Inria Saclay.
- Data Science & Artificial Intelligence DAY – 5eme Edition. 21 October 2021, Paris - Saclay.