Federico Nesti

Via G. Gambini 9
56124 Pisa
Italy

fed.nesti@gmail.com
+39 334 5999455
http://retis.santannapisa.it/~f.nesti/

Federico Nesti

Profile

I am a hard-working and fast-learning **Robotics and Automation Engineer**, with Electronics Engineering background. I work as a **PhD Student** at Scuola Superiore Sant'Anna in Pisa, where I research the limits of physical adversarial examples for convolutional neural networks. I truly believe in a near future where AI and robots will help humans live better lives on a daily basis, and I would love to work to make this happen.

Experience

Visiting Researcher
Universidad de Alicante (RoViT lab), Spain *[Feb. 2022 - Jul. 2022]*
[Benchmarks for evaluation of adversarial robustness in autonomous driving perception]

Consulting Engineer
Scuola Superiore Sant'anna (TeCIP Institute), Pisa *[Jul. 2020 - Ongoing]*
[Architectures and algorithms for train localization systems—Collaboration with Hitachi STS]

Scholarship Holder (Safety for learning-based autonomous systems)
Scuola Superiore Sant'anna (TeCIP Institute), Pisa *[May 2019 - Sep. 2019]*
[Reinforcement Learning, software architectures for predictable and safe Deep Learning]

Robotics R&D Engineer
Fabrica Machinale srl - roboticom, Pisa *[Sep. 2018 - Apr. 2019]*
[Dev.ment of automated procedures for multi-brand industrial robots - EE change, calibration, ...]

Visiting Scientist (M.Sc. Thesis: Eye Tracking for Proton Clinic Environment)
TU Delft (DCSC), Netherlands *[Jan. 2018 - Jun. 2018]*
[Development of an Eye Tracking device - computer vision, machine learning, Bayesian filters]

Internship
Fermilab, Batavia (IL), USA *[Aug. 2017 - Sep. 2017]*
[Automatic position control for automatic magnet centering; pose estimation for solenoids]

Electronics and Control Engineer
U-Phos Project (Rexus-Bexus Programme) *[Sep. 2015 - Jun. 2017]*
[PCB design and test, heating control of device under test]

Skills

Competences (theory)	Computer Vision, Machine/Deep Learning, Control Theory, Navigation, Reinf. Learning
Programming/ SW	Python3, Matlab/Simulink, ROS, Latex, Industrial Robots, C/C++
Deep Learning	PyTorch, Tensorflow1.x
Languages	Italian, English
Other	Traveling, basketball, tennis, guitar et al., hiking, concerts, cooking, and more!

Education

International PhD Student in Emerging Digital Technologies
Scuola Superiore Sant'Anna (TeCIP Institute), Pisa [*October 2019 - Ongoing]*
[Trustworthy Deep Learning, real-world adversarial attacks and defenses]

Deep Learning + Reinforcement Learning Summer School
CIFAR, Mila [*August 2020], Online*
[Reinforcement Learning, Deep Learning]

Computer Vision NanoDegree
Udacity
January 2019 - April 2019

M.Sc. Robotics and Automation Engineering (110/110 cum Laude)
University of Pisa
September 2015 - July 2018

B.Sc. Electronics Engineering (110/110 cum Laude)
University of Pisa
September 2012 - July 2015

Publications

G. Rossolini, F. Nesti et al., *"Defending From Physically-Realizable Adversarial Attacks Through Internal Over-Activation Analysis " [To appear]*

G. Rossolini, F. Nesti et al., *"One the Real-World Adversarial Robustness of Real-Time Semantic Segmentation Models for Autonomous Driving". ArXiv pre-preprint, 2022*

F. Nesti et al., *"Evaluating the robustness of Semantic Segmentation for Autonomous Driving against Real-World Adversarial Patch Attacks".* **2022 IEEE/CVF Winter Conference on Applications of Computer Vision (WACV 2022)**

F. Nesti et al., *"Detecting Adversarial Examples by Input Transformations, Defense Perturbations, and Voting".* **IEEE Transactions on Neural Networks and Learning Systems, 2021**

A. Biondi *et al.* "*A Safe, Secure, and Predictable Software Architecture for Deep Learning in Safety-Critical Systems".* **IEEE Embedded Systems Letters, 2019**

For a complete list of publications, visit my Google Scholar.

PhD Activities and Awards

- "Talento all'Opera" Award (Best PhD Student in EDT from Fondazione "Talento All'Opera")
- 2nd place Huawei University Challenge (expert track)
- 8 hrs of lectures since 2020 in "Deep Learning and Neural Networks" (PhD course by prof. Buttazzo, Scuola Superiore Sant'Anna), on the topics "Neural network-based control" and "Adversarial attacks and defenses"
- Primary reviewer for IEEE Transactions on Neural Networks and Learning Systems and IEEE Transactions on Information Forensics and Security