International Institute for Applied Knowledge Management

KM Conference 2025

25 - 28 June 2025

Department of Information Engineering and Mathematics, University of Siena, Italy

Themes: Knowledge Management, Cybersecurity, Learning, and Information Technology

https://iiakm.org/conference/

Keynote Lecture

Adversarial Examples: Unavoidable Threat or Scarecrow?

Professor Mauro Barni

Professor, Department of Information Engineering and Mathematics
Università di Siena

Keynote Overview:

Since the discovery of adversarial examples, extensive research has been devoted to understanding the underlying vulnerabilities of deep learning models to carefully crafted inputs, and to developing effective countermeasures. Nearly a decade later, it is now clear that adversarial examples ubiquitously affect all types of deep learning models, regardless of their architecture or target task. However, the fundamental reasons for the existence of adversarial examples remain elusive. Significant efforts have also been directed toward designing defenses, most of which have ultimately been circumvented through minor adaptations of the attack algorithms. Nonetheless, attacking real-world applications is far from trivial, since leveraging adversarial examples outside controlled settings presents substantial challenges. By focusing on the case of binary decision networks, this talk aims to propose a possible explanation for why adversarial examples are particularly easy to craft and to shed light on the practical obstacles attackers must overcome to exploit these examples in real-world scenarios.

About the Keynote Presenter:

Mauro Barni is full professor at the University of Siena, where he funded the Visual Information Processing and Protection group (VIPP). In about three decades of activity, he has been studying the application of image and signal processing for security applications. His current research interests include multimedia forensics, adversarial machine learning and DNN watermarking. He published about 350 papers in international journals and conference proceedings. He has been the Editor in Chief of the IEEE Transactions on Information Forensics and Security for the years 2015-2017. He was the funding editor of the EURASIP Journal on Information Security. He has been the chairman of the IEEE Information Forensic and Security Technical Committee (IFS-TC. He was the technical program chair of ICASSP 2014. He was appointed DL of the IEEE SPS for the years 2013-2014. He is the recipient of the Individual Technical Achievement Award of EURASIP for 2016. He is a fellow member of the IEEE, EURASIP and AAIA.