(Global Initiative of Academic Network)

Adversarial Signal Processing and Machine Learning with applications to Multimedia Forensics

(Feb. 14--18, 2022)

Overview

Security-oriented applications of signal processing are receiving increasing attention. Digital watermarking, steganography, multimedia forensics, biometrics, intrusion detection, network monitoring, are just a few. In all these cases, the presence of one or more adversaries aiming at making the system fail cannot be neglected. For each of the above fields, several attacks and counter-attacks have been developed, often following a typical cat & mouse loop wherein attacks and countermeasures are iteratively developed each time focusing on the latest developed solutions. A problem with such an approach is that it fails to provide a unifying view of the challenges that the application of signal processing tools in an adversarial setting poses. Worse than that, the security of the proposed solutions is hardly provable due to the lack of rigorous security models suited to capture the peculiarities of the addressed scenarios. The situation is even more critical when Machine Learning (ML) and Artificial Intelligence (AI) tools are involved. In fact, while the use of ML and AI tools can greatly boost the performance of security-oriented systems, their weakness to adversarial attacks can introduce into the system new security breaches thus compromising its security.

The goal of this course is to introduce the students to the security threats associated to the use of signal processing techniques and AI tools in hostile settings. The course will consist of both lectures and hands-on tutorial wherein the concepts illustrated during the lectures will be exemplified by applying them to some selected topics drawn from multimedia forensics field.

Modules **(Brief Description)**	▪ Introduction to adversarial signal processing and adversarial machine learning ▪ Adversarial signal processing and game theory ▪ Adversarial examples in deep learning ▪ Security by obscurity and attack transferability ▪ Backdoor attacks against deep learning: an emerging threat
You Should **Attend If…**	▪ You are graduate or undergraduate student or doctoral student in Electronics, Computer Science, Electrical, Mathematics, and Statistics. ▪ You are a data scientist/industry person and working with Information Forensics and Security. ▪ You are a faculty from academic institution interested in learning how to do research in Information Forensics and Security and how to apply ML/DL in this field
Fees	**The course will be conducted in ONLINE mode.** The participation fees for taking the course are as follows: **Participants from abroad: US $ 250** **Industry/Research Organizations: Rs. 2,500** **Academic Institutions (Faculty): Rs. 700** **Students (UG/PG/Ph.D.): Rs. 500**

Course Coordinator:

Prof. Manish Okade
Department of ECE,
National Institute of Technology (NIT), Rourkela
Phone: 0661-2462471
Mobile: +91-7008111677
e-mail: okadem@nitrkl.ac.in

.....

GIAN Portal registration

http://www.gian.iitkgp.ac.in/GREGN/index

Course registration Link

https://forms.gle/bzdyo4pA

THE FACULTY

Prof. Mauro Barni is a Fellow of IEEE. He graduated in electronic engineering from the University of Florence in 1991. He received the Ph.D. degree in informatics and telecommunications in 1995. During the last two decades, he has been studying the application of image processing techniques to copyright protection and authentication of multimedia and the possibility of processing signals that have been previously encrypted without decrypting them. Lately, he has been working on theoretical and practical aspects of adversarial signal processing. He has authored or coauthored about 300 articles published in international journals and conference proceedings and holds five patents in digital watermarking and image authentication.

Prof. Manish Okade received his B.E. in Electronics and Communication Engineering from BVBCET, Hubli, Karnataka, M.Tech. in the specialization of Automation and Computer Vision from IIT Kharagpur and Ph.D. in the specialization of Computer Vision and Image Processing, IIT Kharagpur. He has several awards to his credit namely IBM's 'The Great Mind Challenge Award' for mentoring student project, Microsoft India Research Travel Grant Award for his visit to Melbourne, Australia, Early Career Research Award, from SERB, 3 best paper awards for his students work at IEEE Techsym, 2014 and ICORT, DRDO, 2019 and 2021 conferences, member of the high level Indian delegation supported by MHRD, India which visited Tokyo, Japan as part of Sakura Science Exchange Program to establish research collaboration with Japanese Universities etc.