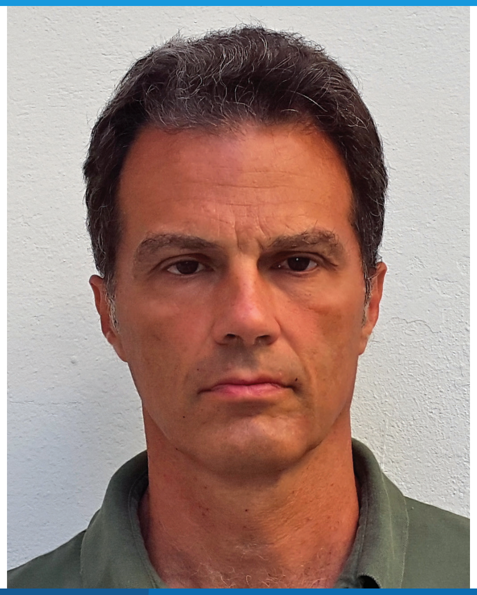
香港浸會大學
HONG KONG BAPTIST UNIVERSITY
計算機科學系
Department of Computer Science

Department of Computer Science
Distinguished Lecture Series 2016/17

Prof. Mauro Barni

Professor, Department of Information Engineering,
University of Siena, Italy



23 May 2017 (Tuesday)
4:30 - 5:30pm

LT1 (SCT501),
Cha Chi-ming Science Tower,
Ho Sin Hang Campus

Adversarial Signal Processing and The Hypothesis Testing Game

Abstract

Security-oriented applications of signal processing have received increasing attention in the last years. Digital watermarking, steganography and steganalysis, multimedia forensics, biometric security, are just a few examples of such an interest. In many cases, though, researchers have failed to recognize the single most unique feature behind any security-oriented application, i.e. the presence of one or more adversaries aiming at making the system fail. One of the most evident consequences is that security requirements are misunderstood, e.g. quite often security is exchanged for robustness. Even when the need to cope with the actions of a malevolent adversary is taken into account, the proposed solutions are often ad-hoc, failing to provide a unifying view of the challenges that such scenarios pose from a signal processing perspective. Times are ripe to go beyond this limited view and lay the basis for a general theory that takes into account the impact that the presence of an adversary has on the design of effective signal processing tools, i.e. a theory of adversarial signal processing. It is the aim of this talk to: i) motivate the need for the development of a general theory of adversarial signal processing; ii) propose a unifying framework based on game-theory; iii) present some recent results regarding adversarial hypothesis testing.

Biography

Mauro Barni received the Electronics Engineering degree from the University of Florence, in 1991, and the Ph.D. degree in informatics and telecommunications in 1995. He has carried out his research activity for over 20 years, first with the Department of Electronics and Telecommunication, University of Florence, and then with the Department of Information Engineering and Mathematics, University of Siena, where he works as Full Professor. 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 (digital watermarking, multimedia forensics, and signal processing in the encrypted domain). Lately, he has been working on theoretical and practical aspects of adversarial signal processing. He participated in several national and European research projects on diverse topics, including computer vision, multimedia signal processing, remote sensing, digital watermarking, and IPR protection. He has authored or coauthored about 300 papers published in international journals and conference proceedings, and is the authors of five patents in the field of digital watermarking and image authentication. He has coauthored the book Watermarking Systems Engineering: Enabling Digital Assets Security and Other Applications (Dekker Inc., 2004). He was the Funding Editor of the EURASIP Journal on Information Security. He is the current Editor-in-Chief of the IEEE TRANSACTIONS ON INFORMATION FORENSICS AND SECURITY. He was the Chairman of the IEEE Information Forensic and Security Technical Committee from 2010 to 2011 and the Technical Program co-Chair of ICASSP 2014. He was appointed as a DL of the IEEE SPS from 2013 to 2014. He is a member of EURASIP and a fellow of IEEE. He was the recipient of the 2016 Individual Technical Achievement of EURASIP.

Enquiry

Tel: 3411-2385 Email: comp@comp.hkbu.edu.hk Website: http://www.comp.hkbu.edu.hk/dlecture/