



UNIVERSITÀ DI PISA
DIPARTIMENTO DI INGEGNERIA DELL'INFORMAZIONE
Dottorato di Ricerca in Ingegneria dell'Informazione

Doctoral Course

“Information Theory and Statistics”

Prof. Mauro Barni

University of Siena – Italy

mauro.barni@unisi.it

Short Abstract: Information theory has been celebrated mostly for its success in modelling information sources and communication systems, however it can be applied to many other application areas always bringing useful and somewhat unexpected insights. The relationship between information theory and statistics is one of such cases. As a matter of fact, some of the most famous results in hypothesis testing and large deviation theory can be revisited from an information theoretic perspective leading to new findings and a deeper understanding of the involved concepts. It is the goal of this course to provide a brief introduction to the use of information theoretic concepts in statistics and, conversely, use some well-known results in statistics to revisit the most celebrated theorems of information theory. In the last part of the course the concepts developed in the first lectures are applied to build a theory of adversarial hypothesis testing, aiming at determining the ultimate achievable performance when hypothesis testing is cast into an adversarial setting encompassing the presence of an adversary aiming at inducing an error in the test. The links of the theory with adversarial machine learning and AI security will be discussed with examples drawn from the multimedia forensics field.

Course Contents in brief:

- Information theory in a nutshell
- The method of types and its relationship with statistics
- Application to large deviation theory and hypothesis testing
- Adversarial hypothesis testing: an information theoretic perspective
- Links with adversarial machine learning and multimedia forensics

Total # of hours of lecture: 18-20

References:

- [1] C. E. Shannon, "A mathematical theory of communication", *Bell system technical journal*, 27(3), 379-423, 1948
- [2] T. M. Cover, J. A. Thomas, "Elements of Information Theory", Wiley Interscience
- [3] M. Barni, B. Tondi, "Lecture notes on: Information Theory and Coding", University of Siena, 2012
- [4] I. Csizar, P. C. Shields, "Information Theory and Statistics: a Tutorial", *Foundations and Trends in Communication and Information Theory*, NOW Publishers Inc., 2004
- [5] B. Tondi, "Theoretical Foundations of Adversarial Detection and Applications to Multimedia Forensics", PhD Thesis, University of Siena, 2016

CV of the Teacher

Mauro Barni graduated in electronic engineering at the University of Florence in 1991. He received the PhD in Informatics and Telecommunications in October 1995. He has carried out his research activity for more than 20 years, first at the Department of Electronics and Telecommunication of the University of Florence, then at the Department of Information Engineering and Mathematics of the University of Siena where he works as full Professor. His activity focuses on digital image processing and information security, with particular reference to the application of image processing techniques to copyright protection (digital watermarking) and authentication of multimedia (multimedia forensics). He has been studying the possibility of processing signals that has been previously encrypted without decrypting them (signal processing in the encrypted domain – s.p.e.d.). Lately he has been working on theoretical and practical aspects of adversarial signal processing.

He is author/co-author of about 300 papers published in international journals and conference proceedings, he holds four patents in the field of digital watermarking and one patent dealing with anticounterfeiting technology. His papers on digital watermarking have significantly contributed to the development of such a theory in the last decade as it is demonstrated by the large number of citations some of these papers have received. The overall citation record of M. Barni amounts to an h-number of 52 according to Scholar Google search engine. He is co-author of the book "Watermarking Systems Engineering: Enabling Digital Assets Security and other Applications", published by Dekker Inc. in February 2004. He is editor of the book "Document and Image Compression" published by CRC-Press in 2006.

He has been the chairman of the IEEE Multimedia Signal Processing Workshop held in Siena in 2004, and the chairman of the IV edition of the International Workshop on Digital Watermarking. He was the technical program co-chair of ICASSP 2014 and the technical program chairman of the 2005 edition of the Information Hiding Workshop, the VIII edition of the International Workshop on Digital Watermarking and the V edition of the IEEE Workshop on Information Forensics and Security (WIFS 2013). In 2008, he was the recipient of the IEEE Signal Processing Magazine best column award. In 2010 he was awarded the IEEE Transactions on Geoscience and Remote Sensing best paper award. He was the recipient of the Individual Technical Achievement Award of EURASIP EURASIP for 2016.

He was the Editor in chief of the IEEE Transactions on Information Forensics and Security from 2015 to 2017. He was the founding editor in chief of the EURASIP Journal on Information Security. He has been a member of the editorial board of several journals including, IEEE Signal Processing Magazine, IEEE Trans. on Circuits and system for Video Technology, IEEE Transactions on

Multimedia, IEEE Signal Processing Letters, the Eurasip Journal of Applied Signal Processing and the IET Proceedings on Information Security.

From 2010 to 2011, Prof. Barni has been the chairman of the IEEE Information Forensic and Security Technical Committee (IFS-TC) of the IEEE Signal Processing Society. He has been a member of the IEEE Multimedia Signal Processing technical committee and of the conference board of the IEEE Signal Processing Society. Mauro Barni is a fellow member of the IEEE and senior member of EURASIP. He was appointed distinguished lecturer by the IEEE Signal Processing Society for the years 2013-2014.

Room and Schedule

Room: *From remote by using Google Meet. The link will be sent in due time to all students who registered to the seminar.*

Schedule:

22,23,25,26 February, 1 March 2021