ECCELLENZA MIUR 2018-2022

ROBOTICS & AI

Sant'Anna
Scuola Universitaria Superiore Pisa

From known knowns to unknown unknowns in AI: Historical and Technical Issues

Scuola Superiore Sant'Anna | Pisa,
Aula Magna 9:00
September 13th, 2022

Speaker:
Prof. Fabio Roli
Università di Genova

Abstract

AI has been originally developed for closed-world, and noise-free, problems where the possible states of natures and actions that a rationale agent could implement were perfectly known. One could argue that, at that time, AI dealt with known knowns. Since the 1980s, when machine learning became an experimental science, AI researchers started to tackle pattern recognition problems with noisy data, using probability theory to model uncertainty and decision theory to minimize the risk of wrong actions. This was the era of known unknowns, characterized by the rise of benchmark data sets, larger and larger year after year, and the belief that real world problems can be solved collecting enough training data. However, recent results have shown that available data sets have often a limited utility when used to train pattern recognition algorithms that will be deployed in the real world. The reason is that modern machine learning has often to face with unknown unknowns. When learning systems are deployed in adversarial environments in the open world, they can misclassify (with high-confidence) never-before-seen inputs that are largely different from known training data. Unknown unknowns are the real threat in many security problems (e.g., zero-day attacks in computer security). In this talk, I give a historical and technical overview of the evolution of AI and machine learning for pattern recognition, and discuss how this evolution can be regarded as a transition from known knowns to unknown unknowns, and the key role that adversarial machine learning plays to make AI safer.

Bio

Fabio Roli received his M.S. degree, with honours, and Ph.D. degree in Electronic Engineering from the University of Genoa, Italy. He was a member of the research group on Image Processing and Understanding of the University of Genoa, Italy, from 1988 to 1994. He was adjunct professor at the University of Trento, Italy, in 1993 and 1994. Since 1995 to 2021, he was with the Dept. of Electrical and Electronic Engineering of the University of Cagliari, Italy, as professor of computer engineering and Director of the PRA Lab. He is now Full Professor at the University of Genova and Founding Director of the PRA Lab. Dr Roli's research activity is focused on the design of pattern recognition systems and their applications to biometric personal identification, multimedia text categorization, and computer security. On these topics, he has published more than three hundred papers at conferences and on journals. He was a very active organizer of international conferences and workshops, and established the popular workshop series on multiple classifier systems. He was a member of the governing boards of the International Association for Pattern Recognition and of the IEEE Systems, Man and Cybernetics Society. He is Fellow of the IEEE, and Fellow of the International Association for Pattern Recognition. He is a recipient of the Pierre Devijver Award for his contributions to statistical pattern recognition.

Contact:
Prof. Alessandro Biondi
alessandro.biondi@santannapisa.it
ph. +39 050882017

Sant'Anna
Scuola Universitaria Superiore Pisa