School of Data Science
香港城市大學
City University of Hong Kong

Hong Kong Institute for Data Science
香港城市大學
City University of Hong Kong

ONLINE SEMINAR

Adversarial Deep Learning in Digital Image Forensics

Date: 3 November 2021 (Wednesday)

Time: 10:00am - 11:00am

Seminar link: https://cityu.zoom.us/j/92747842570

ABSTRACT

In the new AI era, seeing is no longer be believing. Ensuring the integrity and authentication of digital images is increasingly challenging and vital. This talk gives a brief review of my group's research efforts in the intersection of deep learning and digital media security -- adversarial deep learning, including both adversarial attacks and adversarial defenses. Deep learning has achieved state-of-the-art performances in many applications. Unfortunately, both digital images and current deep learning models are vulnerable to manipulations and attacks, giving rise to security, privacy and reliability issues in practical applications.

Under the paradigm of adversarial deep learning, as an attacker, we study potential adversarial attacks and explore novel approaches to study potential vulnerabilities of deep learning models, by investigating three fundamental learning tasks: matching, classification and regression. We present novel attacks (both in the digital domain and in the physical domain) for several essential models belonging to the above three dominant tasks: e.g. GAN-generated fake face imagery forensics; multiclass image classification; camera-LIDAR 3d object detection; and single object tracking in videos. We address the related security threats in the above problems and study how to fool deep learning models to make wrong decisions.

Prof Z. Jane WANG

GUEST SPEAKER'S PROFILE

Prof Z. Jane Wang received the B.Sc. degree from Tsinghua University in 1996 and the M.Sc. and Ph.D. degrees from the University of Connecticut in 2000 and 2002, respectively, all in electrical engineering. She has been Research Associate at the University of Maryland, College Park from 2002 to 2004. Since 2004, she has been with the ECE dept. at the University of British Columbia (UBC), Canada, and she is currently Professor. She is an IEEE Fellow, a Fellow of the Canadian Academy of Engineering (FCAE), and a member of the College of New Scholars, Artists and Scientists of the Royal Society of Canada. Her research interests are in the broad areas of statistical signal processing and machine learning, with current focuses on digital media security and biomedical data analytics. She has been key Organizing Committee Member for numerous IEEE conferences and workshops (e.g., co-Technical Chair for ChinaSIP2014, GlobalSIP2017 and ICIP2021, and co-General Chair of MMSP2018 and DSLW2021). She has been Associate Editor for the IEEE TSP, SPL, TMM, TIFS, TBME, and SPM. She is currently serving as Editor-in-Chief for the IEEE Signal Processing letters.

Enquiries: hkids@cityu.edu.hk

All are welcome