Title: Towards Robust and Safe Machine Learning with Adversarial Training

Abstract: Machine learning (ML), especially deep learning, has achieved great success in many applications. However, recent research investigations show that ML systems are vulnerable on small perturbations of input data, making ML less trustable to be applied in security-critical scenarios. In this talk, we present a unified perspective to build up a robust and safe AI and pattern recognition framework. In particular, we design a minmax adversarial training strategy that has been theoretically justified and empirically validated on many real data. Fundamentals, theories, and applications will be discussed in this talk with intuitive visualizations and numerical verifications. This talk will be mainly based on our research of adversarial training published at ICDM, CVPR, AAAI, ECCV, and ACM Multimedia.

Short Bio: Kaizhu Huang is currently a Professor at the Department of Intelligent Science, Xi’an Jiaotong-Liverpool University, China. He acts as associate dean of research in School of Advanced Technology, XJTLU and is also the founding director of Suzhou Municipal Key Laboratory of Cognitive Computation and Applied Technology. Prof. Huang obtained his PhD degree from Chinese University of Hong Kong (CUHK) in 2004. He worked in Fujitsu Research Centre, CUHK, University of Bristol, National Laboratory of Pattern Recognition, Chinese Academy of Sciences from 2004 to 2012. Prof. Huang has been working in machine learning, neural information processing, and pattern recognition. He was the recipient of 2011 Asia Pacific Neural Network Society Young Researcher Award. He received the best paper or book award six times. So far, he has published 9 books and over 200 international research papers (80+ international journals) e.g., in journals (JMLR, Neural Computation, IEEE T-PAMI, IEEE T-NNLS, IEEE T-BME, IEEE T-Cybernetics, Cognitive Computation) and conferences (NeurIPS, IJCAI, SIGIR, UAI, CIKM, ICDM, ICML, ECML, CVPR). He serves as associated editors/advisory board members in a number of journals and book series. He was invited as keynote speaker in more than 30 international conferences or workshops.