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

ONLINE SEMINAR

Robust Machine Learning in Biometric Recognition

Date: 24 April 2023 (Monday)

Time: 9:00am - 10:00am

Seminar link: https://cityu.zoom.us/j/93672269644

Dr Chun Pong LAU

ABSTRACT

Although deep neural networks have been shown to be successful in various computer vision tasks such as image classification and biometric recognition, robustness and reliability are always the concerns of using deep learning models. On the one hand, degraded images and videos aggravate the performance of biometric recognition. On the other hand, if the deep neural networks are under adversarial attacks, the networks can be broken completely. Motivated by the vulnerability of deep neural networks, I analyze and develop robust biometric recognition including image restoration and adversarial defense algorithms towards a vision of robust machine learning in computer vision.

In this talk, I study two types of degradation making deep neural networks vulnerable. The first part of the talk focuses on face recognition at long range, whose performance is severely degraded by atmospheric turbulence. The theme is on improving the performance and robustness of various tasks in face recognition systems such as face detection, facial keypoints localization, feature extraction, and image restoration. The second part focuses on defending adversarial attacks in the images classification and face recognition tasks. The theme is on exploring adversarial defense methods that can achieve good performance in standard accuracy, robustness to adversarial attacks with known threat models, and good generalization to other unseen attacks.

GUEST SPEAKER'S PROFILE

Dr Chun Pong LAU received the B.Sc. degree in Mathematics at The Chinese University of Hong Kong (CUHK) in 2016, the M.Phil. degree in Mathematics at CUHK in 2018, M.S. degree in Applied Mathematics at University of Maryland, College Park in 2020 and Ph.D. degree in Computer Science at Johns Hopkins University in 2021. He is currently a Mathematical Institute for Data Science Postdoctoral Fellow at Johns Hopkins University. His research interests include image restoration, face recognition, adversarial robustness and generative model. He has published and co-authored several papers in CVPR, NeurIPS, IEEE TIP, IEEE TIFS and IEEE TBIOM. He received the Best Paper (Honorable Mention) award in IEEE FG 2020.

All are welcome

Enquiries: sdscgo@cityu.edu.hk