香港浸會大學理學院
HKBU Faculty of Science

DEPARTMENT OF COMPUTER SCIENCE

PhD Degree Oral Presentation

PhD Candidate:	Mr. Rui SHAO
Date	May 7, 2021 (Friday)
Time:	3:00 pm – 5:00 pm (35 mins presentation and 15 mins Q & A)
Venue:	Zoom ID: 986 1274 0338 (The password and direct link will only be provided to registrants)
Registration:	https://bit.ly/sem-zm (Deadline: 5:00pm, May 5, 2021)

Defense of Face Presentation Attacks and Adversarial Attacks

Abstract

A significant improvement has been achieved in the visual recognition since the advent of deep convolutional neural networks (CNNs). The promising performance in visual recognition has contributed to many real-world visual applications. Face recognition, as one of the most widely used visual applications, even outperforms the human-level recognition accuracy. However, along with convenience brought by the visual applications such as face recognition, many kinds of attacks targeting at them also emerge. Specifically, face presentation attacks (i.e., print attack, video replay attack, and 3D mask attack) can easily fool many face recognition systems. More generally, adversarial attacks which add crafted imperceptible perturbations to clean images can lead general visual recognition systems into making wrong predictions.

In this thesis, we focus on protecting face recognition systems from the face presentation attacks and robustifying general visual recognition systems against the adversarial attacks. Firstly, a multi-adversarial discriminative deep domain generalization framework is proposed to improve the generalization ability of face presentation attack detection method to unseen attacks, which learns a discriminative and shared feature space among multiple source domains via adversarial learning. Secondly, to enable the face presentation attack detection model to learn to generalize well to unseen attacks, a regularized fine-grained meta face presentation attack detection method is proposed, which carries out meta-learning in a variety of simulated domain shift scenarios under face presentation attacks. Apart from defending 2D face presentation attacks, a joint discriminative learning of deep dynamic textures is proposed to capture subtle facial motion differences with spatial- and channel- discriminability for 3D mask presentation attack detection. To exploit the defense against more general adversarial attacks, a new research problem called Open-Set Adversarial Defense (OSAD) is introduced to study the adversarial defense under the open-set setting. An Open-Set Defense Network with Clean-Adversarial Mutual Learning (OSDN-CAML) method is proposed as a solution to the OSAD problem, with the objective of exploiting the complementarity between adversarial robustness and open-set generalization such that the model can simultaneously detect open-set samples and classify known classes in the presence of adversarial noise.

***** ALL INTERESTED ARE WELCOME *****