Zhikai Chen

Address:Xi'An JiaoTong University

Phone: (+86) 13402865893 **Email**: zhikai_chen@outlook.com

EDUCATION

University of Electronic Science and Technology of China, Chengdu, China

Bachelor of Software Engineering

GPA：3.62/4.0 **Overall GPA of Last Two Years**: 3.85/4.0

Xi'An JiaoTong University, Xi'An, China

Master of Software Engineering

Rank： **3rd** in my major

INTERN

Research Intern | Tencent Blade Team Jul. 2020 - till Now

- Testing the Robustness of Face Recognition Systems In Black Box Settings.

Research Intern | Huawei Noah's Ark Lab Jul. 2019 - Jul. 2020

- Studying Robustness of DL Models through Adversarial Examples.
- Using Adversarial Training to help the DL models more robust and gain a more powerful performance.

RESEARCH PROJECTS

Adversarial Attacks on Video Recognition System Jul. 2019 - Nov. 2019

- We are trying to use the information between adjacent frames to generate more powerful adversarial examples.
- We found that make the perturbations with smaller angular distance can enhance the attack ability.

Attacking FaceSwap with Adversarial Perturbations for Defense Nov. 2019 - Apr. 2020

- We can disrupting FaceSwap system by adding imperceptible adversarial perturbations to the source image or target image, the result of normal FaceSwap system can be corrupt.

Defending Deepfakes against Disrupting Images Apr. 2020 - Jul. 2020

- We transfer the disrupting method from facial expression and attribute change model to face swap model.
- We use a compare-based method to make a robust detection, and an elaborate reconstructor to help to deter the adversarial perturbations.

Evaluating Robustness of Video Super-Resolution System Jul. 2020 - Oct. 2020

- We found the adversarial frames can transfer its attack to the adjacent frames, which helps us to propose a more effective method.
- We also do some advanced topics of VSR attack scene(e.g. change the texture of results through modifying the adversarial perturbations).

HONORS AND AWARDS

- 2018-2019 Outstanding Scholarship
- 2017-2018 Outstanding Postgraduate Award
- 2016-2017 National Encouragement Scholarship
- 2017 Challenge Cup national Undergraduate Curricular Academic Science and Technology, Second Prize
- 2015-2016 The Third Prize Scholarship

Publications/Preprints

- Zhikai Chen, Lingxi Xie, Shanmin Pang, Yong He and Qi Tian. Appending Adversarial Frames for Universal Video Attack. Accepted by WACV2021