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 **Outstanding Graduates**

INTERN

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

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

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.

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

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

Black-box Attack on Face Pay System in Physical World Jul. 2020 - Apr.2021

- We propose a query-based attack algorithm that can successfully attack the face IR system.
- We also propose a transfer-based attack method that can successfully attack the face pay system and make an identity theft.

HONORS AND AWARDS

- 2021 Outstanding Graduates
- 2018-2019 & 2019-2020 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
- Zhikai Chen, Lingxi Xie, Shanmin Pang, Yong He and Bo Zhang. MagDR: Mask-guided Detection and Reconstruction for Defending Deepfakes. Accepted by CVPR2021