CHENGUO LIN

Email: linchenguo0622@gmail.com ◇ Homepage: https://chenguolin.github.io/

EDUCATION

B.Eng. in Computer Science, **Sichuan University** Sep. 2018 - Jun. 2022 (expected)

- GPA: 3.91/4.0 Average Score: 93.97/100
- Comprehensive Ranking: 1/171
- Member of Honor College (for top 2% undergraduates at Sichuan University)
- Incoming Ph.D. student in Computer Science at **Peking University**

EXPERIENCES

The University of Hong Kong (HKU) Jun. 2021 - Aug. 2021
Research Intern
Advisor: Prof. Ping Luo
Topic: 3D Visualization of Neural Architecture Search

Korea Advanced Institute of Science and Technology (KAIST) Dec. 2020 - present
Research Assistant
Advisor: Dr. Chaoning Zhang
Topic: Deep Data Hiding, Adversarial Attack

Sichuan University (SCU) Apr. 2019 - Apr. 2020
Undergraduate Research Assistant
Advisor: Prof. Qijun Zhao
Topic: Computer Vision, Forgery of Digital Watermarking

PUBLICATIONS

*: equal contribution

1. Watermark Faker: Towards Forgery of Digital Image Watermarking
   Ruowei Wang*, **Chenguo Lin***, Qijun Zhao, Feiyu Zhu
   IEEE International Conference on Multimedia and Expo (**ICME**), 2021
2. A Survey On Universal Adversarial Attack
   Chaoning Zhang*, Philipp Benz*, **Chenguo Lin***, Adil Karjauv, Jing Wu, In So Kweon
   International Joint Conference on Artificial Intelligence (**IJCAI**), 2021
3. Secure Deep Hiding: Towards Preventing Secret Leakage via Security Key
   Chenguo Lin*, Chaoning Zhang*, Qijun Zhao, In So Kweon
   In Submission
4. A Brief Survey on Deep Learning Based Data Hiding, Steganography and Watermarking
   Chaoning Zhang*, **Chenguo Lin***, Philipp Benz, Kejiang Chen, Weiming Zhang, In So Kweon
   Preprint (**arXiv**)

PROJECTS

- **Universal Deep Hiding with Security Key** Dec. 2020 - present
  It's an extension for the journal version of a NeurIPS2020 paper. We realize a fatal risk of malicious leakage of retrieval module in univeral data hiding and thereby secret messages. Thus, we introduce security key to constitute an additional protective layer for protecting the retrieval module. Extensive experiments are conducted to investigate its performance and mechanism.
- **3D Visualizatino for Neural Architecture Search** Jul. 2021 - Aug. 2021
  To better understand the relationship of different neural architectures in the network coding search space (i.e. various attributions of a network), we developed an interactive front-end system to visualize their relative distribution based on a graph structure.

- **Survey on Universal Adversarial Attack and Deep Data Hiding** Oct. 2020 - Feb. 2021
  We accomplished a brief yet comprehensive survey on universal adversarial perturbations (UAPs), which is accepted by IJCAI2021. Further insight is provided through incorporating the perspective of deep data hiding. We aim to extend this work as a dynamic survey that will regularly update its content to follow new studies.
- **Digital Watermark Forgery Technique Based on Deep Learning** Sep. 2019 - Oct. 2020
  We adopt advanced image generation technique and first shed light on the potential risk caused by forgery of digital watermarking, which is however seriously under-estimated by contemporary researchers. The paper is accepted by ICME2021.

HONORS & AWARDS

- National Scholarship (the highest honor scholarship in China) 2021
- Outstanding Student (Cadre) of Sichuan University 2021, 2020, 2019
- Comprehensive Scholarship of Sichuan University 2020, 2019