

# Jingwen Ye

jingweny@nus.edu.sg | [Github] | [Google Scholar] | LinkedIn

## WORK EXPERIENCE

---

- Research Fellow, National University of Singapore** Nov. 2021 – Present
- Work in LVLab, Department of Electrical and Computer Engineering.
  - Advise Prof. Xinchao Wang on privacy-related machine learning, effective model reuse, and dataset condensation.
- Research Intern, Alibaba Group** Oct. 2017 – Mar. 2019
- Developed a human matting method that was successfully applied in the Taobao APP, resulting in a first-round engagement of 339,187 PV and 82,210 UV.
- Research Intern, Alibaba-Zhejiang University Joint Institute of Frontier Technologies (AZFT)** Jul. 2017 – Sep. 2021
- Proposed the learning algorithm that supported the recommendation system.
  - Received the honor of **Outstanding Intern** in 2019.

## EDUCATION

---

- Ph.D Student, Zhejiang University** Sep. 2016 – Jun. 2021  
College of Computer Science and Technology  
Outstanding Graduate, Advisor: Prof. Chun Chen and Prof. Mingli Song
- B.Eng., Dalian University of Technology** Sep. 2012 – Jun. 2016  
School of Information and Communication Engineering  
Outstanding Graduate, Ranking: 1/35

## SELECTED PUBLICATIONS

---

1. **J. Ye** and X. Wang. “Ungeneralizable Examples.” **CVPR 2024**.
2. **J. Ye**, R. Yu, S. Liu and X. Wang. “Distilled Datamodel with Reverse Gradient Matching.” **CVPR 2024**.
3. **J. Ye**, R. Yu, S. Liu and X. Wang. “Mutual-modality Adversarial Attack with Semantic Perturbation.” **AAAI 2024**.
4. **J. Ye**, S. Liu and X. Wang. “Patial Network Cloning.” **CVPR 2023**.
5. K. Chen et al. “Improving Expressivity of GNNs with Subgraph-specific Factor Embedded Normalization.” **KDD 2023 (Corresponding Author)**.
6. **J. Ye**, Y. Fu, J. Song, X. Yang, S. Liu, X. Jin, M. Song and X. Wang. “Learning with Recoverable Forgetting.” **ECCV 2022**.
7. **J. Ye**, Y. Mao, J. Song, X. Wang, C. Jin, M. Song. “Safe Distillation Box.” **AAAI 2022**.
8. **J. Ye**, Z. Feng and X. Wang. “Flocking Birds of a Feather Together: Dual-step GAN Distillation via Realer-Fake Samples.” VCIP 2022. (**Best Paper**)
9. **J. Ye**, Y. Ji, X. Wang, X. Gao and M. Song. “Data-Free Knowledge Amalgamation via Group-Stack Dual-GAN.” **CVPR 2020**.
10. **J. Ye**, Y. Jing, X. Wang, K. Ou, D. Tao and M. Song. “Edge-Sensitive Human Cutout With Hierarchical Granularity and Loopy Matting Guidance.” **IEEE TIP 2020**.
11. **J. Ye**, Y. Ji, X. Wang, K. Ou, D. Tao and M. Song. “Student Becoming the Master: Knowledge Amalgamation for Joint Scene Parsing, Depth Estimation, and More.” **CVPR 2019**.
12. **J. Ye**, X. Wang, Y. Ji, K. Ou and M. Song. “Amalgamating Filtered Knowledge: Learning Task-customized Student from Multi-task Teachers.” **IJCAI 2019 (Oral)**.
13. **J. Ye**, Z. Feng, Y. Jing and M. Song. “Finer-Net: Cascaded Human Parsing with Hierarchical Granularity.” ICME 2018 (**Oral**).

## ACADEMIC SERVICE

---

Journal Reviewer: TPAMI, TIP, SPM, TCYB, TCSVT, PR, TMLR, ...

Conference Reviewer: CVPR, ICCV, ECCV, ICLR, NeurIPS, ICML, AAAI, IJCAI, ...

## RESEARCH INTEREST

---

My current research interests are mainly about **privacy-related transfer learning** and **effective model reusing**. Specially, I focus on the privacy issues on the AIGC models. Also I investigate deeper with knowledge distillation and amalgamation techniques to improve the performance of the multi-task networks.

## AWARDS AND HONORS

---

Best Paper Award of International Conference on Visual Communications and Image Processing	2022
Outstanding Graduate of Zhejiang Province	2021
National Scholarship (top 2%); Graduate of Merit/Triple A Graduate	2019 & 2020
Excellent Intern of Alibaba-Zhejiang University Joint Research Institute of Frontier Technoligise	2020
Candidate of Chu Kochen Scholarship (top 1%)	2019
Most Valuable Academic Award of Doctoral Forum	2019
Excellent Social Practice Individual Award	2018
Award of Honor for Graduate	2017 & 2018
Outstanding Graduate of Liaoning Province	2016

## PROJECTS

---

<b>Privacy-related Knowledge Transfer</b>	2021 – Present
<ul style="list-style-type: none"><li>• Develop the LIRF framework that explicitly allows for knowledge deposit and withdrawal, to achieve recoverable knowledge forgetting.</li><li>• Develop a novel framework, termed as Safe Distillation Box, allowing to wrap a pre-trained model in a virtual box, which precludes unauthorized KDs while strengthens authorized ones.</li><li>• <b>Five first-author papers</b> have been accepted to CVPR, ECCV and AAAI.</li></ul>	
<b>Adversarial Attack to Self-driving Systems</b> (AISG Project with Continental and Fraunhofer)	2022 – 2024
<ul style="list-style-type: none"><li>• Propose a patch-based attack generation framework for effectively attack the self-driving systems while ensuring the transferability of the attack.</li><li>• Simulate the attack in real world e.g. sticker on the stop sign, and then test and proof it.</li></ul>	
<b>Efficient GAN Training</b>	2020 – 2021
<ul style="list-style-type: none"><li>• Bring forward a general-purpose compression framework for reducing the scale of the generator with the least or none performance degradation.</li><li>• A discriminator is constructed based on the realer-fake sets to minimize the teacher and the student distributions in different groups.</li></ul>	
<b>Knowledge Transfer from Model Zoo</b>	2019 – 2020
<ul style="list-style-type: none"><li>• Propose an innovative knowledge amalgamation strategy for training a compact student using heterogeneous-task teachers specializing in different domains.</li><li>• Extend it to data-free amalgamation by utilizing the knowledge media that collects the amalgamated knowledge into the GAN and then passes it through to TargetNet.</li><li>• Extend it to self-amalgamation by the hybrid distillation objective composed of self/mutual/outer-distillation objectives to facilitate the training of the student model under no external supervision.</li></ul>	