



# KEMOU LI<sup>ID</sup>

Ph.D. Student @ University of Macau

[Google Scholar] [Homepage]

+853 62517633

kemou.li@connect.umac.mo

N21-5006, University of Macau

## EDUCATION

### University of Macau

Ph.D. in Computer Science

- Supervisor: Prof. Jiantao Zhou

2024 – Present

Macao, China

### University of Macau

M.Sc. in Artificial Intelligence Applications (Research Track)

- Supervisor: Prof. Jiantao Zhou
- Master Thesis: *Regroup Median Loss for Combating Label Noise*

2021 – 2023

Macao, China

### Sun Yat-sen University

B.Sc. in Mathematics and Applied Mathematics

- Supervisor: Prof. Zhiwei Wu
- Bachelor Thesis: *The Representation of Lie Algebra of  $G_2$ -Type and Associated Integrable Functions*

2017 – 2021

Guangzhou, China

## RESEARCH EXPERIENCE

### Research Assistant / Intern

State Key Laboratory of Internet of Things for Smart City (SKL-IoTSC), University of Macau

Aug. 2021 – Present

Macao, China

## RESEARCH INTERESTS

**Trustworthy Machine Learning:** LLM Unlearning, Adversarial Training, Learning with Noisy Labels  
**AI Security and Forensics:** Forgery Detection, Backdoor Learning, Membership Inference

## PUBLICATIONS (\* = EQUAL CONTRIBUTION)

### Preprints

- **LLM Unlearning with LLM Beliefs**   
Kemou Li, Qizhou Wang, Yue Wang, Fengpeng Li, Jun Liu, Bo Han, Jiantao Zhou  
*arXiv preprint*, submitted to ICLR-26

### Conferences & Journals

- **Toward Robust Deep Learning via Core Feature-aware Adversarial Training**   
Fengpeng Li\*, Kemou Li\*, Haiwei Wu, Jinyu Tian, Jiantao Zhou  
*IEEE Transactions on Information Forensics and Security (TIFS)*, 2025 [CCF A]
- **RML++: Regroup Median Loss for Combating Label Noise**   
Fengpeng Li, Kemou Li, Qizhou Wang, Bo Han, Jinyu Tian, Jiantao Zhou  
*International Journal of Computer Vision (IJCV)*, 2025 [CCF A]
- **FontGuard: A Robust Font Watermarking Approach Leveraging Deep Font Knowledge**   
Kahim Wong, Jicheng Zhou, Kemou Li, Yain-Whar Si, Xiaowei Wu, Jiantao Zhou  
*IEEE Transactions on Multimedia (TMM)*, 2025 [Tsinghua A]
- **DAT: Improving Adversarial Robustness via Generative Amplitude Mix-up in Frequency Domain**   
Fengpeng Li, Kemou Li, Haiwei Wu, Jinyu Tian, Jiantao Zhou  
*In The 38th Annual Conference on Neural Information Processing Systems (NeurIPS-24)*, 2024 [CCF A]
- **Regroup Median Loss for Combating Label Noise**   
Fengpeng Li, Kemou Li, Jinyu Tian, Jiantao Zhou  
*In The 38th AAAI Conference on Artificial Intelligence (AAAI-24)*, 2024 [CCF A] [Oral, 2.2%]

## Under Review

- **Editprint: General Digital Image Forensics via Editing Fingerprint with Self-Augmentation Training**  
Haiwei Wu, **Kemou Li**, Yuanman Li, Jiantao Zhou  
Submitted to *CVPR-26*
- **AEGIS: Adversarial Target-Guided Retention-Data-Free Robust Concept Erasure from Diffusion Models**  
Fengpeng Li, **Kemou Li**, Qizhou Wang, Bo Han, Jiantao Zhou  
Submitted to *ICLR-26*
- **CASCADE: Coarse-to-Fine Conformal Backdoor Detection in Multimodal Contrastive Learning**  
Yiming Chen, **Kemou Li**, Haiwei Wu, Jiantao Zhou  
Submitted to *IEEE TIFS*
- **Evading Passive Image Forensics via Source Trace Modeling and Attentive Adversarial Manipulation**  
Haiwei Wu, Fengpeng Li, **Kemou Li**, Yuanman Li, Jiantao Zhou, Cong Wang  
Submitted to *IEEE TDSC*

## AWARDS & HONORS

**Inclusion·The Global Multimedia Deepfake Detection (Image Track)** (*Organized by Ant Group*) **Sept. 2024**  
🏆 1st Place (1/706), JTGroup Team. [\[NEWS\]](#) *Prize: 100,000 CNY*

## TEACHING EXPERIENCE

### Teaching Assistant

*Department of Computer and Information Science, Faculty of Science and Technology, University of Macau*

- [GEST1009] (G) Multimedia Technology in Modern Society, Fall 2025
- [CISC7202] (PG) Tools for Machine Learning, Spring 2025
- [CISC7014] (PG) Advanced Topics in Computer Science (Image Processing and Pattern Recognition), Fall 2024

## PROFESSIONAL SERVICES

### Journal Reviewer

- IEEE Transactions on Information Forensics and Security (*TIFS*)

### Conference Reviewer / Program Committee

- Conference on Computer Vision and Pattern Recognition (*CVPR*), 2026
- International Conference on Learning Representations (*ICLR*), 2026
- Conference on Neural Information Processing Systems (*NeurIPS*), 2025
- International Conference on Machine Learning (*ICML*), 2025
- Asia-Pacific Signal and Information Processing Association Annual Summit and Conference (*APSIPA ASC*), 2024–2025

## TECHNICAL SKILLS

**Programming:** Python, PyTorch, LaTeX

**Languages:** English (*fluent*), Mandarin (*native*), Teochew (*native*), Cantonese (*basic*)