YISHAN LI

College of Systems Engineering, National University of Defense Technology, Changsha, China

liyishan@nudt.edu.cn • yishanli226@gmail.com • (+86) 182-2988-8307 • Date of Birth: Feb 26, 1999

Research Interests

Digital watermarking for generative AI and multimedia security; adversarial machine learning; safety of large language models; self-supervised and contrastive learning.

Education

National University of Defense Technology (NUDT), Changsha, China **Sep 2024 – Present**
Ph.D. candidate in Management Science and Engineering. GPA: 3.75/4

National University of Defense Technology (NUDT), Changsha, China **Sep 2021 – Jun 2024**
M.Eng. in Electronic Information (Artificial Intelligence).

Jilin University, Changchun, China **Sep 2017 – Jun 2021**
B.Eng. in Road, Bridge and River-Crossing Engineering.

Publications

†: *equal contribution* *: *corresponding author*

[1] Yishan Li, Yanming Guo*, Yulun Wu, et al., "RDAT: an efficient regularized decoupled adversarial training mechanism," *International Journal of Multimedia Information Retrieval*, 2024, 13(2): 24.

[2] Yishan Li, Yanming Guo*, Yuxiang Xie, et al., "A Survey of Defense Methods Against Adversarial Examples," in *International Conference on Big Data and Information Analytics (BigDIA)*, IEEE, 2022: 453–460.

[3] Yishan Li, Tianjian Zhou, Mingrui Lao, Pan Liu, and Yanming Guo *, "TextSeal: Content-Binding Watermarks for Detecting Phrase-Level Rendered-Text Tampering," under review.

[4] Yishan Li, Tianjian Zhou, Mingrui Lao, and Yanming Guo *, "Parameter-Geometry Watermarking for LoRA-Adapted JEPA-Style Predictive World Models," under review.

[5] Yishan Li, Tianjian Zhou, and Jinxian Wang *, "PASS: A Keyed Identity Read Inside Vision-Language Models," under review.

[6] Yishan Li, Tianjian Zhou, Xuankun Rong, Mingrui Lao, Wenke Huang, Yanming Guo*, and Mang Ye, "Semantic Cluster Parity for Multi-bit LLM Watermarking," under review.

[7] Jiangfan Liu† and **Yishan Li**†, Yanming Guo*, et al., "Generation and Countermeasures of adversarial examples on vision: a survey," *Artificial Intelligence Review*, 2024, 57(8): 199.

[8] Tianjian Zhou†, **Yishan Li**†, Jie Jiang*, Liang Bai, and Yifei Zhang, "CMAE: Contrastive Manifold Autoencoder for Efficient Latent Diffusion," *IEEE International Conference on Multimedia and Expo*

(*ICME*), 2026.

[9] Tianjian Zhou, Jie Jiang, **Yishan Li***, Yifei Zhang, "DAGA: Dynamic Attention-Guided Adaptation for Self-Supervised Vision Transformers," *Conference on Neural Information Processing Systems* (*NeurIPS*), *2026.*

[10] Tianjian Zhou, **Yishan Li**, Lixin Zhan, and Jie Jiang*, "Less is More: Minimal Components for Contrastive Learning Delivering Superior Accuracy and Efficiency," *IEEE Trans. Neural Networks and Learning Systems* (*TNNLS*), 2026.

[11] Tianjian Zhou, Jie Jiang*, **Yishan Li**, Lixin Zhan, Rui Qi, and Liang Bai, "Semantic-guided data augmentation for self-supervised visual pattern learning: Leveraging foundation model priors," *Pattern Recognition*, 2026.

[12] Tianjian Zhou, **Yishan Li**, Lixin Zhan, and Jie Jiang*, "HTNet: A self-supervised heterogeneous triple network for multi-modal data," *Neural Networks*, 2026.

[13] Yunhao Feng, Yanming Guo*, Mingrui Lao, Yulun Wu, **Yishan Li**, and Yuxiang Xie, "FCAT: Federated causal adversarial training," *Knowledge-Based Systems*, 2025, 330: 114440.

Patents

[P1] "Adversarial training and image classification method based on decoupled consistency regularization," Chinese invention patent application, No. 202411300867.9 (filed, 2nd inventor).

[P2] "Method and devices for generating multi-class targeted adversarial examples," Chinese invention patent granted 2023, CN114078201B (5th inventor).

Research Projects

- **Adaptive Defense against Unknown Adversarial Attacks**, National Natural Science Foundation of China (NSFC), No. 72571281, 2026–. Participant: co-drafted the proposal; implementing the technical solution of the third subtask.
- **Robust and Efficient Adaptive Adversarial Training for Adversarial Scenarios**, Hunan Provincial Natural Science Foundation, No. 2025JJ40066, 2025–. Participant: co-wrote the proposal; implemented the algorithms of the first two subtasks.
- **Adversarial Attack and Robust Defense Technologies for Intelligent Algorithms**, Changsha Municipal Science and Technology Project, No. kq2209001, 2022–2024. Participant: prepared the proposal and technical reports; implemented the second optimization algorithm and its deployment.

Honors and Awards

- Second Prize, CICC Science and Technology Progress Award (first student contributor), 2025
- Excellence Award, 1st National Intelligent Algorithm Adversarial Competition, 2025

- Third Prize, 7th "Huawei Cup" China Graduate AI Innovation Competition, 2025
- Second Prize, 6th "Huawei Cup" China Graduate AI Innovation Competition, 2024
- Second Prize (team leader), Asia and Pacific Mathematical Contest in Modeling (APMCM), 2024
- Third Prize, 12th MathorCup University Mathematical Modeling Challenge, 2022

Experience

Algorithm Engineer Intern, Hunan Advanced Research Institute **Mar 2023 – Jun 2023**
Research on intelligent adversarial applications for target recognition: adversarial example generation and defense.