9 Wenyuan Road, Nanjing
Jiangsu Province, 210023

Jin Song

(86) 182 0196 3248
JinSongResearch@outlook.com

Education

Nanjing University of Posts and Telecommunications **Nanjing, CN**
B.S.E in Information Security *Fall 2022 – Fall 2026*

- Undergraduate in Information Security, GPA: 3.9 / 5.0
- Member of AnHeng Elite Program [Supported by DBAPP Security Co., Ltd.].
- President of Student Science Association.

Publications

- Yuan Yao, **Jin Song**, Jian Jin. (ACM CCS 2025 under review)
  Hashed Watermark as a Filter: Boosting Robustness of Weight-based Neural-Network Watermarking
- Yuan Yao, **Jin Song**, Yu Zhang, Jian Jin (NeurIPS 2025 under review)
  Semi-Supervised Noise Adaptation: Transferring Knowledge from Noise Domain
- Jiaqi Wu, Yuan Yao, **Jin Song**, Simin Chen, Rui Jing, Lixu Wang, Zehua Wang, Zijian Tian, Wei Chen, Jian Jin. (NeurIPS 2025 under review)
  Rethinking Client Knowledge for Federated Learning: An Entangled Representation Perspective

Research Experiences

Hashed Filter for White-box Watermark **Dec/2023 - Sep/2024**

Supervisor: Lixin Fan, Yuan Yao

- Uncovered hypothetical details that were neglected in previous studies and came up with augmented overwriting attacks.
- Proposed NeuralMark: a model watermark system combining hash function with filter mechanism to block the chance of ambiguity attack and lower the risk of parameter overlapping, improving robustness against augmented overwriting attack.
- Implemented NeuralMark on 11 image classification architectures and 2 text generation architectures with LoRA.
- Conducted fidelity experiments on 6 datasets and compared NeuralMark with 3 state-of-the-art (SOTA) watermark system.
- Demonstrated robustness of NeuralMark through 4 different attack experiments on 4 datasets.
- Analyzed the effectiveness of NeuralMark under different circumstances through 3 controlled experiments and the interference of NeuralMark to the original task through 6 additional controlled analysis experiments.
- Wrote the theoretical proof presented in the manuscript that demonstrates how the hash chain in NeuralMark mitigates the probability of a successful ambiguity attack.

Noise Adaptation for Semi-Supervised Learning **Sep/2024 - May/2025**

Supervisor: Yu Zhang, Yuan Yao

- Utilized the classical domain adaptation theory to demonstrate the feasibility of noise adaptation.
- Explored the role of noise in facilitating learning and proposed the Noise Adaptation Framework(NAF), which aligns the noise domain(modality) with the semi-supervised domain(modality) to improve the semi-supervised performance.
- Conducted controlled experiments across 5 benchmark datasets and compared it with Empirical Risk Minimization.
- Coupled NAF with the current state-of-the-art (SOTA) method and compared it with the results obtained without coupling.
- Analyzed the effectiveness of NAF through 6 controlled analysis experiments.

Representation Entanglement for Federated Learning **Jan/2025 - May/2025**

Collaborator: Yuan Yao, Jiaqi Wu

- Proposed a writing perspective centered on the proposal of the concept of Representation Entanglement.
- Participated in the review and writing of the manuscript.

Honors & Awards

Rank 90/706, Inclusion - The Global Multimedia Deepfake Detection (2024)

- Performed offline image augmentation for the minority positive samples and online augmentation for the majority negative samples, thereby improving the diversity of the official unbalanced dataset.
- Tried various image classification architectures and hyperparameters for 1 epoch and choose EfficientNet-B1 as the final model due to memory constraints of Kaggle platform.

Rank 129/772, The 2nd World AI4S Prize-Logical Reasoning Track Evaluation of complex reasoning ability (2024)

- Utilized Test Time Scaling(Majority Vote) and Prompt Engineering to improve the accuracy of Qwen2-7B-Instruct API.

Rank 74 / 449, Alibaba Cloud Tianchi College Student Competition (2024)

Third Prize, 14th "Lanqiao Cup" National Competition for Software and Information Technology (2023)

Third Prize, The 28th University Science and Technology Festival 'BIT Cup' Challenge (2023)

Second Prize, The 25th 'Innovation Cup' University Student Extracurricular Academic and Technological Works Competition (2023)

Third Prize, The 2nd University Student Programming Competition (2022)

Extracurricular Experiences

- Distinguished Group Leader of the Summer Study Tour at NTU(2024)
- Examiner of Institute Theoretical Application Logic Competition(2024)
- Student of Datawhale AI Summer Camp (2024)
- Teaching Assistant of Datawhale AI Campus Tour (2024)
- Participant of AWS Summit Shanghai (2024)
- Student of Trusted Federated Learning Winter Camp - Westlake University (2023)
- Judge of the Student Science Association Freshmen Recruitment (2023)

Skills & Interests

- **Technical Skills:** Python, PyTorch, C/C++, Linux, Latex, Markdown.
- **Interests:** Multimodal Machine Learning, Reinforcement Learning, Embodied AI, Game Design.
- **Hobbies:** Tennis, Video Game, Music, Photography, Traveling.

Language

- **TOEFL:** 102 [2025].