Zhongliang Guo

Email: zg34@st-andrews.ac.uk| Homepage| Google Scholar

Technology Stack

Areas of Expertise:	AI Robustness, Adversarial Sample, Computer Vision
Programming Language:	Python, JAVA, SQL, C#, JavaScript, LaTeX, HTML5
Libraries & Frameworks:	PyTorch, Diffusers, OpenCV, NumPy, Pandas, Matplotlib, Django
Tools & Technologies:	Linux, Shell, Vim, Slurm, Docker, Git

Education

PhD ***Computer Science***, University of St Andrews, *Full scholarship with stipend*, Supervisor: Oggie and Lei 2022 - Now
MSc ***Artificial Intelligence*** with **Distinction**, University of St Andrews, Nominated on 2021/2 *Deans' List* 2021 - 2022
BSc ***Forensic Science***, NWUPL, GPA: 88.4/100 (ranked 1/55), Awarded 2021 Outstanding UG Dissertation 2017 - 2021

Selected Publication & Patent

*equal contribution †corresponding author oral session poster session

- **Zhongliang Guo**, Yifei Qian, Shuai Zhao, Junhao Dong, Yanli Li, Ognjen Arandjelović, Fang Lei, and Chun Pong Lau. Artwork Protection Against Unauthorized Neural Style Transfer and Aesthetic Color Distance Metric. ***Pattern Recognition***, 2025.
- **Zhongliang Guo**†, Yifei Qian, Kaixuan Wang, Weiye Li, Ziheng Guo, Yuheng Wang, Yanli Li, Ognjen Arandjelović, and Lei Fang. Artwork Protection Against Neural Style Transfer Using Locally Adaptive Adversarial Color Attack. In *The 27th European Conference on Artificial Intelligence* (**ECAI 2024**), volume 392, pages 1414–1421. IOS Press, 2024.
- **Zhongliang Guo**†, Weiye Li, Yifei Qian, Ognjen Arandjelovic, and Lei Fang. A White-Box False Positive Adversarial Attack Method on Contrastive Loss-Based Offline Handwritten Signature Verification Models. In *The 27th International Conference on Artificial Intelligence and Statistics* (**AISTATS 2024**), volume 238, pages 901–909. PMLR, 2024.
- **Zhongliang Guo**†, Ognjen Arandjelović, David Reid, Yaxiong Lei, and Jochen Büttner. A Siamese Transformer Network for Zero-Shot Ancient Coin Classification. ***Journal of Imaging***, 9(6):107, 2023.
- **Zhongliang Guo**, Dian Jia, Zhaokai Wang, and Yongqi Zhou. A Method of Video Recognition Network of Face Tampering Based on Deep Learning, **A.U. Patent** 2019101186A4, Oct. 2019.
- Yanli Li, **Zhongliang Guo**, Nan Yang, Huaming Chen, Dong Yuan, and Weiping Ding. Threats and Defenses in Federated Learning Life Cycle: A Comprehensive Survey and Challenges. *IEEE Transactions on Neural Networks and Learning Systems* (**IEEE T-NNLS**), 2025.
- Yifei Qian, **Zhongliang Guo**, Bowen Deng, Chun Tong Lei, Shuai Zhao, Chung Pong Lau, Xiaopeng Hong, and Michael P Pound. T2ICount: Enhancing Cross-modal Understanding for Zero-Shot Counting. In **CVPR 2025 Highlight**, 2025.
- Chun Tong Lei, Hon Ming Yam, **Zhongliang Guo**, Yifei Qian, and Chun Pong Lau. Instant Adversarial Purification with Adversarial Consistency Distillation. In **CVPR 2025**, 2025.
- Yifei Qian, Xiaopeng Hong, **Zhongliang Guo**, Ognjen Arandjelović, and Carl R Donovan. Semi-Supervised Crowd Counting with Masked Modeling: Facilitating Holistic Understanding of Crowd Scenes. *IEEE Transactions on Circuits and Systems for Video Technology* (**IEEE T-CSVT**), 34(9):8230–8241, 2024.
- Yifei Qian, Liangfei Zhang, **Zhongliang Guo**, Xiaopeng Hong, Ognjen Arandjelović, and Carl R Donovan. Perspective-assisted Prototype-based Learning for Semi-supervised Crowd Counting. ***Pattern Recognition***, page 111073, 2024.
- Shuai Zhao, Meihuizi Jia, **Zhongliang Guo**, Leilei Gan, Xiaoyu Xu, Xiaobao Wu, Jie Fu, Feng Yichao, Fengjun Pan, and Anh Tuan Luu. A Survey of Recent Backdoor Attacks and Defenses in Large Language Models. ***Transactions on Machine Learning Research***, 2025. **Survey Certification**.
- Man Hu, Yatao Yang, Deng Pan, **Zhongliang Guo**, Luwei Xiao, Deyu Lin, and Shuai Zhao. Syntactic paraphrase-based synthetic data generation for backdoor attacks against Chinese language models. ***Information Fusion***, 2025.
- Ziheng Guo, **Zhongliang Guo**, Ognjen Arandjelović, and Andrea di Falco. Generative Model for Multiple-Purpose Inverse Design and Forward Prediction of Disordered Waveguides in Linear and Nonlinear Regimes. In ***Machine Learning in Photonics***, volume 13017, page 1301702. SPIE, 2024.
- **Zhongliang Guo**, Lei Fang, Jingyu Lin, Yifei Qian, Shuai Zhao, Zeyu Wang, Junhao Dong, Cunjian Chen, Ognjen Arandjelović, and Chun Pong Lau. A Grey-box Attack against Latent Diffusion Model-based Image Editing by Posterior Collapse. ***Under review***, 2024.

Academic Work Experience

1. **Senior Research Fellow at University of Lancaster** (Grade 8, funded by the UKRI MRC) Apr 2024 - Now
   - **Postdoc Researcher**. Line manager is Dr Sophie Nightingale.
   - Develop machine learning methods to prevent ordinary people from Deepfakes.
   - Develop web crawler to build a comprehensive Deepfake dataset.
   - Provide academic guidance to junior colleagues.
2. **Research Collaboration with City University of Hong Kong** Apr 2024 - Now
   - **Technical Mentor**. Serve as a technical mentor for Prof. Chun Pong Lau's lab.
   - Provid academic guidance to **3 first-year PhD students** on adversarial attack/defense and diffusion-based generation.
   - Participate in research ideation sessions, helping to conceptualize and validate experimental approaches.
   - Contribute to 1 paper in **CVPR 2025**, two papers in writing.
3. **Research Fellow at University of St Andrews** (Grade 5.23, funded by **Tapoly**) Jan 2025 - Mar 2025
   - **Principal Investigator**. LLM based chatbot for insurance industry.
   - Design the architecture of **AI chatbot** for domain-specific Q&A.
   - Conduct **RAG** system to ensure more accurate answer and do not need to fine-tune the backbone model.
4. **Research Fellow at University of St Andrews** (Grade 5.23, funded by **MathWorks**) Dec 2023 - Nov 2024
   - **Principal Investigator**. Machine Learning based drone and bird radar detection using micro-Doppler radar signature.
   - Design and implement **physical models** to simulate avian and drone dynamics.
   - Conduct **field experiments** to collect various radar frequency data of birds and drones.
   - Process data into corresponding micro-Doppler images and creating a **new dataset**.
   - Develop multiple usage neural network for bird-drone-clutter-noise **classification** and moving **object tracking**.
5. **Teaching Assistant** (Covers UG level and PGT level) Sep 2023 - Now
   - Modules include CS1002 OOP, CS3105 AI, and ID5059 KDD.
   - Topic covers **Java**, **Search**, **Games**, **Uncertainty**, and **Machine Learning**.
   - Demonstrate lab session, mark coursework.

Research Experience

1. **Adversarial Attack for Social Good**
   - **Principal Investigator**. Explore the benign use of adversarial attack in terms of computer vision.
   - Propose an adversarial pre-processing method to protect artwork from **unauthorized neural style transfer**, allowing artists to safeguard their unique style against popular transfer techniques.
   - Propose a near **black-box** attack method against **Latent Diffusion Models**, achieving **SOTA** performance at 4× faster than existing approaches; aiming to defend against malicious use of Latent Diffusion Model-based image editing techniques.
2. **Adversarial Attack for AI Robustness**
   - **Principal Investigator**. Explore the vulnerability of existing machine learning models and potential defenses.
   - Expose the **illusory robustness** in SOTA **signature verification** models, proposing a False Positive attack to address the unbalanced performance of existing attack methods.
   - Propose an efficient attack framework against **multi-modal diffusion models**, utilizing distilled backbones and optimized noise predictors to generate high-fidelity adversarial examples with superior transferability and robustness against defenses.
   - Propose a **one-step** diffusion-based **adversarial purification** method using controlled purification and noise distillation, achieving **rapid** and **robust** defense against various attacks.
3. **Deepfakes Detection and Defense**
   - **Principal Investigator**. Explore using algorithms to detect and defense deepfakes.
   - Propose a **multi-scale hybrid architecture** as the backbone model to boost detecting images tampered by deepfakes.
   - Propose a **adversarial attack**-based method to prevent deepfakes, which will significantly disrupt the output of Deepfakes.

Honor & Grant

	Date
• 2021 NWUPL Outstanding Undergraduate Dissertation	Jun 2021
• 2021/2022 Dean's List at University of St Andrews	Sep 2022
• 2022 - 2026 full PhD scholarships with stipend	Oct 2022
• ECAI 2024 Conference Travel Grant from EurAI (22 out of 547)	Oct 2024
• CVPR 2025 Highlight Paper (Top 3%)	Jun 2025