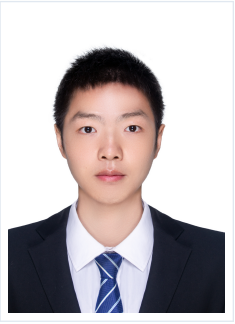
Language / 语言： Chinese 中文 | English 英文



聂何望

讲师 / 网络与信息安全教研室

广西师范大学（2025.07–至今）

nhw@gxnu.edu.cn | (+86)185-8983-1671 | 中国 • 广西桂林

导航：

简介

聂何望，男，汉族，籍贯江西省九江市，博士/讲师。2025 年 6 月毕业于华中科技大学，获网络与信息安全博士学位。长期致力于人工智能安全、可逆信息隐藏、神经网络模型水印等领域的研究。主持中央网信办创新资助计划项目，参与国家重点研发计划、国家科学自然基金地区科学基金项目、广西高校中青年教师基础能力提升项目等重要科研项目研究。已在国内外著名期刊和会议发表论文十余篇，其中 SCI 一区 top 国际期刊论文 5 篇、CCF-B 类国际期刊/会议论文 6 篇，获授权发明专利 3 件，软件著作权 1 件。担任 IEEE TAI，IPM，KBS，ESWA，EAAI，Neural Networks，Information Fusion，ICASSP 等国际著名期刊、会议审稿人。

研究方向

- 人工智能安全、神经网络模型版权保护
- 多媒体信息安全、神经网络水印、可逆信息隐藏、图像水印
- 联邦学习安全、模型所有权验证

教育背景

- 华中科技大学，博士，网络与信息安全，导师：路松峰（2021.09–2025.07）
- 广西师范大学，硕士，软件工程，导师：唐振军（2017.09–2020.07）
- 广西科技大学，学士，软件工程，导师：阳树洪（2013.09–2017.07）

工作经历

- 广西师范大学，专任教师（2025.07–至今）
- 广西科技师范学院，专任教师（2020.07–2021.01）

学术任职

- “新一代图像安全技术研讨会”——程序委员会委员（Program Committee Member）

审稿人

担任以下期刊/会议审稿人（含长期服务期刊）：

- **期刊：** IEEE Transactions on Artificial Intelligence；IEEE Access；Knowledge-Based Systems；Expert Systems with Applications；Engineering Applications of Artificial Intelligence；Information Processing & Management；Information Fusion；Information Sciences；Applied Soft Computing；Neural Networks；Neurocomputing；Signal Processing；Ad Hoc Networks；Cluster Computing；Complex & Intelligent Systems；EURASIP Journal on Image and Video Processing；IET Image Processing；PLOS ONE；Journal of King Saud University – Computer and Information Sciences；Smart Health；Computer Law & Security Review；International Journal of Computational Intelligence Systems 等
- **会议：** ICASSP；IEEE International Joint Conference on Neural Networks (IJCNN) 等

科研项目

- 中央网络安全和信息化委员会办公室，网络安全学院学生创新资助计划，AI 数据模型防泄露检测工具，2024.04–2025.04，5 万元，结题，主持

- 国家重点研发计划，2021YFB2012200，开放式数控系统安全可信技术，2021.11–2024.10，2297 万元，结题，参与
- 广西壮族自治区教育厅，广西高校中青年教师基础能力提升项目，2021KY0861，基于注意力卷积神经网络的目标检测算法研究，2021.01–2025.04，2 万元，结题，参与
- 国家自然科学基金地区科学基金项目,61962008,基于矩阵分解的彩色图像哈希算法研究,2020.01.01–2023.12.31，40 万元，结题，参与

论文发表

说明：姓名后标注†为**通讯作者**；姓名后标注*为**共同一作**。

期刊论文（按年份）

2025

1. **Hewang Nie**, Xuemei Yuan. *Compression Is No Barrier: Dataset Copyright Protection with Compression-Resistant Backdoor Watermarks.* Information Processing & Management (中科院一区 TOP, CCF B), 2025.
2. Xuemei Yuan, **Hewang Nie**†. *Beyond Protection: Unveiling Neural Network Copyright Trading.* Knowledge-Based Systems (中科院一区 TOP, CCF C), 2025.
3. Xuemei Yuan, **Hewang Nie**†. *Secure Industrial Federated Learning: Label Encryption for Model Protection.* Engineering Applications of Artificial Intelligence (中科院一区 TOP, CCF C), 2025.
4. Jue Xiao*, **Hewang Nie***, Xueming Tang, Songfeng Lu. *Federated Learning with Bilateral Defense via Blockchain.* Neural Networks (中科院二区, CCF B), 2025.

2024

1. **Hewang Nie**, Songfeng Lu, Junjun Wu, Jianxin Zhu. *Deep Model Intellectual Property Protection with Compression-Resistant Model Watermarking.* IEEE Transactions on Artificial Intelligence, 2024.
2. **Hewang Nie**, Songfeng Lu. *PersistVerifty: Federated model ownership verification with spatial attention and boundary sampling.* Knowledge-Based Systems (中科院一区 TOP, CCF C), 2024.
3. **Hewang Nie**, Songfeng Lu. *FedCRMW: Federated model ownership verification with compression-resistant model watermarking.* Expert Systems with Applications (中科院一区 TOP, CCF C), 2024.
4. **Hewang Nie**, Songfeng Lu. *Securing IP in Edge AI: Neural Network Watermarking for Multimodal Models.* Applied Intelligence (中科院三区, CCF C), 2024.

2020

1. Zhenjun Tang, **Hewang Nie**, Chi-Man Pun, Heng Yao, Chunqiang Yu, Xianquan Zhang. *Color image reversible data hiding with double-layer embedding.* IEEE Access (中科院四区), 2020.

会议论文（按年份）

2025

1. Hao Fei*, **Hewang Nie***, Siqi Sun, Songfeng Lu, Ting Luo, Dunbo Cai, Zhiguo Huang, Runqing Zhang. *Optimized Dynamic Watermarking for Audio DNNs with Adaptive Embedding and Boundary Sampling*. ICASSP 2025 (CCF B).
2. Jue Xiao, Zepu Yi, **Hewang Nie**, Zhi Lu, Xueming Tang, Songfeng Lu, Zhiguo Huang, Runqing Zhang. *FedDiT: Federated Learning by Distillation Token Enhanced Vision Transformer*. ICASSP 2025 (CCF B).

2024

1. **Hewang Nie**, Songfeng Lu, Mu Wang, Jue Xiao, Zhi Lu, Zepu Yi. *VeriChroma: Ownership Verification for Federated Models via RGB Filters*. Euro-Par 2024 (CCF B).
2. Zhi Lu, Songfeng Lu, Yongquan Cui, Junjun Wu, **Hewang Nie**, Jue Xiao, Zepu Yi. *Lightweight Byzantine-Robust and Privacy-Preserving Federated Learning*. Euro-Par 2024 (CCF B).

发明专利

- 路松峰, 路直,**聂何望**, 杨豪. 一种基于国产密码的工控数据安全防护系统及其工作方法. CN118133298A (2024).
- 路松峰, 周立天, 朱建新, 罗勇,**聂何望**. 一种基于 LSTM 的数控系统日志审计方法及终端. CN116781321A (2023).
- 路松峰, 肖珏, 路直,**聂何望**, 杨豪. 一种适用于数控系统的流加密机及其工作方法. CN116684076A (2023).

软件著作权

- **聂何望**, 唐振军, 凌曼, 广西师范大学. 基于 SVM 的车牌识别软件 V1.0，登记号：2018SR219059

学术交流

- **2025-11-21 至 2025-11-23，海南海口**：第六届 *CSIG* 中国媒体取证与安全大会（The 6th CSIG Chinese Conference on Media Forensics and Security, ChinaMFS 2025）。主办方：中国图象图形学学会；承办方：CSIG 数字媒体取证与安全专委、海南大学、《网络空间安全科学学报》。
- **2025-11-07 至 2025-11-09，广西桂林**：新一代图像安全技术研讨会（Workshop on New-Generation Image Security Technologies）。主办方：广西师范大学**计算机科学与工程学院 /**

软件学院 / 人工智能学院。

- **2024-08-26 至 2024-08-30，西班牙马德里**：*Euro-Par 2024：第 30 届并行与分布式计算国际欧洲大会*（Euro-Par 2024: 30th International European Conference on Parallel and Distributed Computing）。主办方：Euro-Par 2024 组委会（马德里当地承办单位）。
- **2019-10-18 至 2019-10-20，福建厦门（北海湾惠龙万达嘉华酒店）**：*第十五届全国信息隐藏暨多媒体信息安全学术大会*（The 15th China Information Hiding and Multimedia Security Workshop, CIHW 2019）。主办方：中国电子学会通信分会、北京电子技术应用研究所；承办方：清华大学、华侨大学。

荣誉奖项

- 优秀毕业博士研究生（2025）
- 国家奖学金（2023–2024）

教学与指导

开设课程：

指导研究生

-

指导本科生

- 高锐（2019 级）：全国蓝桥杯大赛广西赛区三等奖。
- 韩林荣（2019 级）：全国蓝桥杯大赛广西赛区二等奖。

办公地点

办公地址：广西师范大学育才校区 文二楼 503 室
办公时间：工作日 9:00–17:30（或邮件预约）

招生启事

欢迎对人工智能安全、联邦学习与模型水印等方向感兴趣的同学报考与加入课题组！

同时欢迎踏实勤奋、积极上进的本科生加入本课题组。

- **研究方向：**模型版权保护、联邦学习所有权验证、数据/模型水印、AI 安全评测等
- **期望背景：**具备良好的编程基础（Python/PyTorch 优先），对科研有热情与自驱力
- **联系方式：**请附个人简历、成绩单、代表性成果（如有）发送至：nhw@gxnu.edu.cn

联系方式

- 邮箱：nhw@gxnu.edu.cn
- 电话：(+86)185-8983-1671
- 所在地：中国 • 广西桂林

Go to English version / 跳转到英文版

Hewang Nie

Lecturer / Cyberspace Security Teaching & Research Section

Guangxi Normal University (Jul. 2025–Present)

nhw@gxnu.edu.cn | (+86)185-8983-1671 | Guilin, Guangxi, China

Navigation:

About

Hewang Nie is a Lecturer with a Ph.D. in Cyberspace Security from Huazhong University of Science and Technology (June 2025). His research focuses on AI security, reversible information hiding, and neural network watermarking. He has led a student innovation funding project from the Cyberspace Administration of China and participated in major research programs including the National Key R&D Program of China, the National Natural Science Foundation of China (regional fund), and the Guangxi University Young and Middle-aged Teachers' Basic Ability Improvement Project. He has published over ten papers in well-known journals and conferences, including five papers in SCI Q1 (TOP) journals and six papers in CCF-B journals/conferences. He holds three granted invention patents and one software copyright. He serves as a reviewer for international journals and conferences such as IEEE TAI, IPM, KBS, ESWA, EAAI, Neural Networks, Information Fusion, and ICASSP.

Research Interests

- AI security; intellectual property protection for neural network models
- Multimedia information security; neural network watermarking; reversible information hiding; image watermarking
- Federated learning security; model ownership verification

Education

- Ph.D., Cyberspace Security, Huazhong University of Science and Technology; Advisor: Songfeng Lu (2021.09–2025.07)
- M.Eng., Software Engineering, Guangxi Normal University; Advisor: Zhenjun Tang (2017.09–2020.07)
- B.Eng., Software Engineering, Guangxi University of Science and Technology; Advisor: Shuhong Yang (2013.09–2017.07)

Experience

- Lecturer, Guangxi Normal University (2025.07–present)
- Lecturer, Guangxi Science and Technology Normal University (2020.07–2021.01)

Academic Service

- *Workshop on New-Generation Image Security Technologies* —Program Committee Member

Reviewer

Reviewer for (including long-term service):

- **Journals:** IEEE Transactions on Artificial Intelligence; IEEE Access; Knowledge-Based Systems; Expert Systems with Applications; Engineering Applications of Artificial Intelligence; Information Processing & Management; Information Fusion; Information Sciences; Applied Soft Computing; Neural Networks; Neurocomputing; Signal Processing; Ad Hoc Networks; Cluster Computing; Complex & Intelligent Systems; EURASIP Journal on Image and Video Processing; IET Image Processing; PLOS ONE; Journal of King Saud University – Computer and Information Sciences; Smart Health; Computer Law & Security Review; International Journal of Computational Intelligence Systems, etc.
- **Conferences:** ICASSP; IEEE International Joint Conference on Neural Networks (IJCNN), etc.

Projects

- Cyberspace Administration of China, Student Innovation Funding (Cybersecurity School): *AI Data/Model Leakage Detection Tool*, 2024.04–2025.04, CNY 50,000, completed, PI
- National Key R&D Program of China, 2021YFB2012200: *Security and Trustworthiness for Open CNC Systems*, 2021.11–2024.10, CNY 22.97M, completed, participant
- Guangxi Zhuang Autonomous Region Education Department, Young and Middle-aged Teachers' Basic Ability Improvement Project, 2021KY0861: *Object Detection with Attention-based CNN*, 2021.01–2025.04, CNY 20,000, completed, participant
- National Natural Science Foundation of China (Regional Fund), 61962008: *Color Image Hashing via Matrix Factorization*, 2020.01.01–2023.12.31, CNY 400,000, completed, participant

Publications

Note: † = corresponding author; ∗ = co-first author.

Journal Articles (by year)

2025

1. **Hewang Nie**, Xuemei Yuan. *Compression Is No Barrier: Dataset Copyright Protection with Compression-Resistant Backdoor Watermarks.* Information Processing & Management (CAS Q1 TOP, CCF B), 2025.
2. Xuemei Yuan, **Hewang Nie**†. *Beyond Protection: Unveiling Neural Network Copyright Trading.* Knowledge-Based Systems (CAS Q1 TOP, CCF C), 2025.
3. Xuemei Yuan, **Hewang Nie**†. *Secure Industrial Federated Learning: Label Encryption for Model Protection.* Engineering Applications of Artificial Intelligence (CAS Q1 TOP, CCF C), 2025.
4. Jue Xiao∗, **Hewang Nie**∗, Xueming Tang, Songfeng Lu. *Federated Learning with Bilateral Defense via Blockchain.* Neural Networks (CAS Q2, CCF B), 2025.

2024

1. **Hewang Nie**, Songfeng Lu, Junjun Wu, Jianxin Zhu. *Deep Model Intellectual Property Protection with Compression-Resistant Model Watermarking.* IEEE Transactions on Artificial Intelligence, 2024.
2. **Hewang Nie**, Songfeng Lu. *PersistVerifty: Federated model ownership verification with spatial attention and boundary sampling.* Knowledge-Based Systems (CAS Q1 TOP, CCF C), 2024.
3. **Hewang Nie**, Songfeng Lu. *FedCRMW: Federated model ownership verification with compression-resistant model watermarking.* Expert Systems with Applications (CAS Q1 TOP, CCF C), 2024.
4. **Hewang Nie**, Songfeng Lu. *Securing IP in Edge AI: Neural Network Watermarking for Multimodal Models.* Applied Intelligence (CAS Q3, CCF C), 2024.

2020

1. Zhenjun Tang, **Hewang Nie**, Chi-Man Pun, Heng Yao, Chunqiang Yu, Xianquan Zhang. *Color image reversible data hiding with double-layer embedding.* IEEE Access (CAS Q4), 2020.

Conference Papers (by year)

2025

1. Hao Fei*, **Hewang Nie***, Siqi Sun, Songfeng Lu, Ting Luo, Dunbo Cai, Zhiguo Huang, Runqing Zhang. *Optimized Dynamic Watermarking for Audio DNNs with Adaptive Embedding and Boundary Sampling.* ICASSP 2025 (CCF B).
2. Jue Xiao, Zepu Yi, **Hewang Nie**, Zhi Lu, Xueming Tang, Songfeng Lu, Zhiguo Huang, Runqing Zhang. *FedDiT: Federated Learning by Distillation Token Enhanced Vision Transformer.* ICASSP 2025 (CCF B).

2024

1. **Hewang Nie**, Songfeng Lu, Mu Wang, Jue Xiao, Zhi Lu, Zepu Yi. *VeriChroma: Ownership Verification for Federated Models via RGB Filters.* Euro-Par 2024 (CCF B).
2. Zhi Lu, Songfeng Lu, Yongquan Cui, Junjun Wu, **Hewang Nie**, Jue Xiao, Zepu Yi. *Lightweight Byzantine-Robust and Privacy-Preserving Federated Learning.* Euro-Par 2024 (CCF B).

Patents

- Songfeng Lu, Zhi Lu, **Hewang Nie**, Hao Yang. *Industrial Control Data Security Protection System and Method based on Chinese Cryptography.* CN118133298A (2024).
- Songfeng Lu, Litian Zhou, Jianxin Zhu, Yong Luo, **Hewang Nie**. *Log Audit Method and Terminal for CNC Systems based on LSTM.* CN116781321A (2023).
- Songfeng Lu, Jue Xiao, Zhi Lu, **Hewang Nie**, Hao Yang. *Stream Cipher Device and Method for CNC Systems.* CN116684076A (2023).

Software Copyright

- **Hewang Nie**, Zhenjun Tang, Man Ling, Guangxi Normal University. *License Plate Recognition Software V1.0 based on SVM.* Registration No.: 2018SR219059

Academic Exchanges

- **Nov 21–23, 2025, Haikou, Hainan, China:** *The 6th CSIG Chinese Conference on Media Forensics and Security (ChinaMFS 2025).* Organizer: China Society of Image and Graphics (CSIG); Co-organizers: CSIG TC on Digital Media Forensics and Security, Hainan University, *Journal of Cyber Security Science*.
- **Nov 7–9, 2025, Guilin, Guangxi, China:** *Workshop on New-Generation Image Security Technologies.* Organizer: College of Computer Science and Engineering, School of Software, and School of Artificial Intelligence, Guangxi Normal University.
- **Aug 26–30, 2024, Madrid, Spain:** *Euro-Par 2024: 30th International European Conference on Parallel and Distributed Computing.* Organizer: Euro-Par 2024 Organizing Committee (local hosts in Madrid).
- **Oct 18–20, 2019, Xiamen, Fujian, China (Beihai Bay Huilong Wanda Realm Hotel):** *The 15th China Information Hiding and Multimedia Security Workshop (CIHW 2019).* Organizers: Communication Society of China Electronics Society & Beijing Institute of Electronic Technology Application; Co-organizers: Tsinghua University & Huaqiao University.

Honors

- Outstanding Graduating Ph.D. Student (2025)
- National Scholarship (2023–2024)

Teaching

Courses offered:

Graduate Supervision

-

Undergraduate Supervision

- Rui Gao (Class of 2019): Third Prize, LanQiao Cup (Guangxi Division).
- Linrong Han (Class of 2019): Second Prize, LanQiao Cup (Guangxi Division).

Office

Address: Room 503, Wen Building 2, Yucai Campus, Guangxi Normal University
Office Hours: Weekdays 9:00–17:30 (or by email appointment)

Admission

We welcome motivated students interested in AI security, federated learning, and model watermarking to join our group.

Diligent and proactive undergraduates are also welcome to join the group.

- **Research Topics:** Model IP protection, federated model ownership verification, data/model watermarking, AI security evaluation
- **Preferred Background:** Solid programming skills (Python/PyTorch preferred) and strong research motivation
- **How to Apply:** Please email your CV, transcript, and representative work (if any) to nhw@gxnu.edu.cn.

Contact

- Email: nhw@gxnu.edu.cn
- Phone: (+86)185-8983-1671
- Location: Guilin, Guangxi, China