

导师简介：刘勇，男，博士，硕士研究生导师，中国图像图形学会会员，主要从事人工智能安全、人工智能内容安全等方面的研究工作。近年来，主持湖北省自然科学基金青年项目1项、十堰市重点实验室开放基金项目1项，参与国家重点研发计划项目1项、国家自然科学基金面上项目2项、腾讯犀牛鸟基金项目1项，在国内外重要期刊和会议上共发表论文10余篇，担任CCF A期刊和会议审稿人。



研究方向：多媒体内容安全、人工智能安全、AIGC内容安全

教授课程：人工智能语言及算法、自然语言处理、人工智能基础

邮 箱：liuyong@huat.edu.cn

工作经历：

1. 湖北汽车工业学院 讲 师 2024.10-至今

近年来主要科研项目：

1. 湖北省科技厅，基于频域可解释的神经网络模型水印研究，湖北省自然科学基金青年项目，2025-03-01至2027-02-28，主持
2. 湖北汽车工业学院，黑盒神经网络鲁棒水印研究，电磁感应与节能技术十堰市重点实验室开放基金项目，2024-06 至 2026-06，主持
3. 国家自然科学基金委员会，数字文创资产发行与流通应用示范，国家重点研发计划项目，2023-11至2026-10，参与
4. 国家自然科学基金委员会，以神经网络模型为载体的安全隐写研究，国家自然科学基金面上项目，2024-01至2027-12，参与
5. 腾讯公司和中国计算机学会，多媒体水印及取证新方法研究，CCF-腾讯犀牛鸟基金项目，参与

近年来代表性论文：

- [1] **Liu Yong**, Wu Hanzhou, Zhang Xinpeng. Robust and Imperceptible Black-box DNN Watermarking Based on Fourier Perturbation Analysis and Frequency Sensitivity Clustering[J]. IEEE Transactions on Dependable and Secure Computing, 2024, 21(6): 5766-5780. (SCI, CCF A)
- [2] **Liu Yong**, Zhang Li, Wu Hanzhou, Wang Zichi, Zhang Xinpeng. Reducing High-Frequency Artifacts for Generative Model Watermarking via Wavelet Transform[J]. IEEE Internet of Things Journal, 2024, 11(10): 18503-18515. (SCI, 一区TOP)
- [3] Yang Wei, **Liu Yong**, Chen Yi, Cui Yunhe, Guo Chun. HSMNet: A multi-resolution grayscale image steganalysis method based on hybrid dilated convolution and self-attention multi-channel network[J]. Information Sciences, 2025: 122824. (SCI, 一区TOP)
- [4] Qiu Xin, Shi Canghong, Li Xiaojie, Wu Min, M. Abdullahi Sani, **Liu Yong**. S-Faster R-CNN: Intra-Spectral Similarity Learning for Audio Copy-Move Forgery Localization in IoT Security[J]. IEEE Internet of Things Journal, 2025, 12(15):30185 - 30202. (SCI, 一区TOP)
- [5] Chen Yi, Wang Hongxia, Cui Yunhe, Guo Chun, **Liu Yong**, Wu Hanzhou. A multi-level additive distortion method for security improvement in palette image steganography[J]. Journal of Visual Communication and Image Representation, 2025, 110: 104463. (SCI, 三区)

招生情况说明：

欢迎对人工智能安全和生成式人工智能内容安全感兴趣的同学加入课题组，优秀学子可推荐进入川大、电子科大、中科大等高校攻读博士。