Yunming Zhang

Email: YMZhang97@outlook.com | Tel: +86 195-1015-2879 | Date of Birth: Feb 26, 1997 | Wuhan University

Academic Homepag: scholar.google.com/citations?user=K5kUms0AAAAJ

Research Interests: Multimedia deep watermarking, Deepfake Defense, Multimedia Forensics

Education Background

Wuhan University, School of Cyber Science and Engineering, Key Laboratory of Aerospace Information Security and Trusted Computing Ministry of Education — Sep 2022 – Now

- Ph.D candidate in Cyberspace Security
- Supervisor: Prof. Dengpan Ye

Shandong Normal University, School of Information Science and Engineering Information and Communication Engineering — Sep 2019 – Jun 2022

- M.S. in Information and Communication Engineering
- Supervisor: Assoc. Prof. Wenbo Wan and Prof. Jiande Sun

Taishan University, School of Physics and Electronic Engineering — Sep 2015 – Jun 2019

- B.S. in Communication Engineering

Research Projects and Competitions

Projects

- National Natural Science Foundation of China (NSFC), Research on General Robust Adversarial Example Theory and Methods for Secure Image Steganography Applications. — 2022–2024
- National Natural Science Foundation of China (NSFC), Image Watermarking Based on Robust Multilevel Perception Feature. — 2019-2020
- National Natural Science Foundation of China (NSFC), Research on Information Hiding Technology Based on CoverVideo Selection. — 2019-2022
- China Postdoctoral Science Foundation, Research on High Performance Image Watermarking Method Based on Visual Perception. — 2019-2022

Competition

- Huawei Cup National Graduate Cyber Security Innovation Competition, First Prize — Nov 2023

Awards

National Scholarship	Oct 2024
Second Prize Scholarship of Wuhan University	Oct 2024
Excellent Graduate Student of Wuhan University	Oct 2024
Outstanding Individual of Wuhan University	Jan 2024
Second Prize Scholarship of Wuhan University	Oct 2023
Excellent Master's Thesis of Shandong Normal University	Jun 2022
National Scholarship	Oct 2021
Third Prize Scholarship of Shandong Normal University	Oct 2020
Excellent Graduate Student of of Shandong Normal University	Oct 2020

Publications

†: equal contribution author ∗:corresponding author

Under review/preprint

- StyleMark: A Robust Watermarking Method for Art Style Images Against Black-Box Arbitrary Style Transfer
  Yunming Zhang, Dengpan Ye∗, Sipeng Shen, Jun Wang , Xi Xiao , Yongdong Wu
  2025 AAAI Conference, under review, 2024.
- DIP-Watermark: A Double Identity Protection Method Based on Robust Adversarial Watermark
  Yunming Zhang, Dengpan Ye∗, Caiyun Xie, Sipeng Shen , Ziyi Liu, Jiacheng Deng, Long Tang
  IEEE Transactions on Dependable and Secure Computing, under review, 2024 arxiv.org/abs/2404.14693

Published

- Dual defense: Adversarial, traceable, and invisible robust watermarking against face swapping
  Yunming Zhang, Dengpan Ye∗, Caiyun Xie, Long Tang , Xin Liao, Ziyi Liu, Chuanxi Chen, Jiacheng Deng
  IEEE Transactions on Information Forensics and Security, 2024,19: 4628-464. 10.1109/TIFS.2024.3383648
- Once and for All: Universal Transferable Adversarial Perturbation against Deep Hashing-Based Facial Image Retrieval
  Long Tang, Dengpan Ye∗, Yunna Lv, *Chuanxi Chen* , Xin Liao, Ziyi Liu, Chuanxi Chen, ***Yunming Zhang***
  Proceedings of the AAAI Conference on Artificial Intelligence , 2024. 10.1609/aaai.v38i6.28319
- Feature Extraction Matters More: An Effective and Efficient Universal Deepfake Disruptor
  Long Tang, Dengpan Ye∗, Zhenhao Lu, ***Yunming Zhang*** , Xin Liao, Ziyi Liu, Chuanxi Chen, Jiacheng Deng
  ACM Transactions on Multimedia Computing, Communications and Applications , 2024. 10.1145/3653457
- AVT2-DWF: Improving Deepfake Detection with Audio-Visual Fusion and Dynamic Weighting Strategies
  Rui Wang, Dengpan Ye∗, Long Tang, ***Yunming Zhang*** , Jiacheng Deng
  IEEE Signal Processing Letter, 2024. 10.48550/arXiv.2403.14974
- Towards Perceptual Image Watermarking with Robust Texture Measurement
  Yunming Zhang, Yuxin Gong, Jun Wang, Jiande Sun , Wenbo Wan∗
  Expert Systems with Applications, 2023, 219(1):119649. 10.1016/j.eswa.2023.119649
- A Comprehensive Survey on Robust Image Watermarking
  Wenbo Wan†, Jun Wang† ,***Yunming Zhang***, Jing Li, Hui Yu∗,Jiande Sun∗
  Neurocomputing, 2022, 488: 226-247. 10.1016/j.neucom.2022.02.083
- JND-Aware Robust Image Watermarking with Tri-directional Inter-block Correlation
  Yunming Zhang, Zhenhua Wang, Yantong Zhan, Lili Meng , Jiande Sun , Wenbo Wan∗
  International Journal of Intelligent Systems, 2021, 36(12): 7053-7079. 10.1002/int.22580
- Spatial-Perceptual Embedding with Robust Just noticeable Difference model for color Image Watermarking
  Kai Zhou, ***Yunming Zhang***, Jing Li , Yantong Zhan, Wenbo Wan∗
  Mathematics, 2020, 8(9): 1506. 10.3390/math8091506