Han Fang, Ph.D.

Contact Information

Research Fellow, School of Computing
National University of Singapore, Singapore

℗: +65-83097184
✉: fanghan@nus.edu.sg

Research Interests

Digital Watermarking, Adversarial Machine Learning.

Working Experiences

National University of Singapore, Singapore

Research Fellow, Oct 2021 - Current
Under the supervision of Prof. Ee-Chien Chang
School of Computing

Education Experiences

University of Science and Technology of China, Hefei, China

Ph.D., Sep 2016 - Jun 2021
School of Cyber Science and Technology

- Adviser: Prof. Weiming Zhang and Prof. Nenghai Yu
- Area of Study: Image Watermarking

Nanjing University of Aeronautics and Astronautics, Nanjing, China

B.E., Sep 2012 - Jun 2016
College of Electronic and Information Engineering

Accepted Papers (Selected)

[1] **H. Fang**, K. Chen, Y. Qiu, J. Liu, K. Xu, C. Fang, W. Zhang and E. Chang. DeNoL: A Few-Shot-Sample-Based Decoupling Noise Layer for Cross-channel Watermarking Robustness. *Proceedings of the 31th ACM International Conference on Multimedia (ACM MM)*, 2023.

[2] **H. Fang**, J. Zhang, Y. Qiu, J. Liu, K. Xu, C. Fang and E. Chang. Tracing the Origin of Adversarial Attack for Forensic Investigation and Deterrence. *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)*, 2023.

[3] **H. Fang**, Y. Qiu, K. Chen, J. Zhang, W. Zhang and E. Chang. Flow-Based Robust Watermarking with Invertible Noise Layer for Black-Box Distortions. *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI)*, 2023.

[4] **H. Fang**, Z. Jia, Z. Ma, E. Chang and W. Zhang. PIMoG: An Effective Screen-shooting Noise-Layer Simulation for Deep-Learning-Based Watermarking Network. *Proceedings of the 30th ACM International Conference on Multimedia (ACM MM)*, 2022.

[5] **H. Fang**, Y. Qiu, Q. Guo, J. Zhang, K. Chen, W. Zhang and E. Chang. DP^2: Dataset Protection by Data Poisoning. *IEEE Transactions on Dependable and Secure Computing (TDSC)*, 2022.

[6] **H. Fang**, Z. Jia, Y. Qiu, J. Zhang, W. Zhang and E. Chang. De-END: Decoder-driven Watermarking Network. *IEEE Transactions on Multimedia (TMM)*, 2022.

[7] **H. Fang**, Z. Jia, H. Zhou, W. Zhang and N.Yu. Encoded Feature Enhancement in Watermarking Network for Distortion in Real Scenes. *IEEE Transactions on Multimedia (TMM)*, 2022.

[8] **H. Fang**, D. Chen, F. Wang, Z. Ma, H. Liu, W. Zhou, W. Zhang and N.Yu. TERA: Screen-to-camera Image Code with Transparency, Efficiency, Robustness and Adaptability. *IEEE Transactions on Multimedia (TMM)*, 2021.

[9] **H. Fang**, D. Chen, Q. Huang, J. Zhang, Z. Ma, W. Zhang and N.Yu. Deep Template-based Watermarking. *IEEE Transactions on Circuits and Systems for Video Technology (TCSVT)*, 2020.

[10] **H. Fang**, W. Zhang, Z. Ma, H. Zhou, S. Sun, H. Cui and N.Yu. A Camera Shooting Resilient Watermarking Scheme for Underpainting Documents. *IEEE Transactions on Circuits and Systems for Video Technology (TCSVT)*, 2019.

[11] **H. Fang**, W. Zhang, H. Zhou, H. Cui and N.Yu. Screen-shooting Resilient Watermarking. *IEEE Transactions on Information Forensics and Security (TIFS)*, 2018.

[12] **H. Fang**, H. Zhou, Z. Ma, W. Zhang and N. Yu. A robust image watermarking scheme in DCT domain based on adaptive texture direction quantization. *Multimedia Tools and Applications*, 2019.

[13] J. Zhao, **H. Fang*** and W. Zhang. MBRS: Enhancing Robustness of Dnn-based Watermarking by Mini-batch of Real and Simulated JPEG Compression. *Proceedings of the 29th ACM International Conference on Multimedia (MM)*, 2021. (***Corresponding Author**)

[14] C. Liu, J. Zhang, **H. Fang***, Z. Ma, W. Zhang and N. Yu. DeAR: A Deep-learning-based Audio Re-recording Resilient Watermarking. *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI)*, 2023. (***Corresponding Author**)

[15] X. Yang, J. Zhang, **H. Fang***, C. Liu, Z. Ma, W. Zhang and N. Yu. AutoStegaFont: Synthesizing Vector Fonts for Hiding Information in Documents. *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI)*, 2023. (***Corresponding Author**)

[16] H. Zhou, K. Chen, W. Zhang, **H. Fang**, W. Zhou and N. Yu. Dup-net: Denoiser and upsampler network for 3d adversarial point clouds defense. *Proceedings of the IEEE/CVF International Conference on Computer Vision (ICCV)*, 2019.

[17] J. Zhang, D. Chen, J. Liao, **H. Fang**, W. Zhang, W. Zhou, H. Cui and N. Yu. Model watermarking for image processing networks. *Proceedings of the AAAI Conference on Artificial Intelligence (AAAI)*, 2020.

[18] Z. Ma, W. Zhang, **H. Fang**, X. Dong, L. Geng and N. Yu. Local Geometric Distortions Resilient Watermarking Scheme Based on Symmetry. *IEEE Transactions on Circuits and Systems for Video Technology (TCSVT)*, 2021.

[19] X. Yang, W. Zhang, **H. Fang**, Z. Ma and N. Yu. Language Universal Font Watermarking with Multiple Cross-media Robustness. *Signal Processing*, 2023.

[20] Z. Ma, X. Yang, **H. Fang**, W. Zhang and N. Yu. OAcode: Overall Aesthetic 2D Barcode on Screen. *IEEE Transactions on Multimedia (TMM)*, 2023.

[21] L. Geng, W. Zhang, H. Chen, **H. Fang** and N. Yu. Real-time Attacks on Robust Watermarking Tools in the Wild by CNN. *Journal of Real-Time Image Processing*, 2020.

[22] F. Wang, H. Zhou, **H. Fang**, W. Zhang and N. Yu. Noise Simulation-Based Deep Optical Watermarking. *Artificial Intelligence and Security: 8th International Conference*, 2022.

PROFESSIONAL SERVICE

- Reviewer of some top-tier conferences and journals, including CVPR, ICCV, AAAI, MM, TNNLS, TMM.