Basic Information

Name：	Yunshu Dai	Country：	China
Gender：	Female	Birth Date：	1998.01.02
Phone：	15295732188	Email：	daiyunshu0102@163.com

Education

	Doctor of Engineering	**Master of Engineering**	**Bachelor of Engineering**
Institution	Sun Yat-sen University, China	Nanjing University of Information Science and Technology, China	Nanjing University of Information Science and Technology, China
Major	Cyber Science and Technology	Computer Science and Technology	Material Physics

Publication

1. **Y. Dai**, J. Fei and F. Huang, C. Chang, Robust Secure Swap: Responsible Face Swap With Persons of Interest Redaction and Provenance Traceability, In Proceedings of the 42th International Conference on Machine Learning (ICML 2025), Vancouver, Canada.
2. **Y. Dai,** J. Fei and F. Huang, IDGuard: Robust, General, Identity-Centric POI Proactive Defense Against Face Editing Abuse, 2024 IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2024), Seattle, WA, USA, 2024, pp. 11934-11943.
3. **Y. Dai**, J. Fei，F. Huang and Z. Xia, Face Omron Ring: Proactive defense against face forgery with identity awareness, Neural Networks, Volume 180, 2024,106639, ISSN 0893-6080.
4. J. Fei*, **Y. Dai***，P. Yun, T. Shen, Z. Xia, J. Weng. Learning Second Order Local Anomaly for General Face Forgery Detection. Proceedings of the IEEE/CVF Conference on Computer Vision and Pattern Recognition (CVPR 2022), New Orleans, USA, 2022, pp. 20270-20280.
5. **Y. Dai,** J. Fei, H. Wang, Z. Xia. Attentional Local Contrastive Learning for Face Forgery Detection. International Conference on Artificial Neural Networks. Springer, Cham, 709-721, 2022.09.07.
6. Fei, J., **Y. Dai**, Xia, Z., Huang, F., & Zhou, J. OmniMark: Efficient and Scalable Latent Diffusion Model Fingerprinting. Proceedings of the AAAI Conference on Artificial Intelligence (AAAI 2025), 39(16), 16550-16558.
7. W. Huang, **Y. Dai,** J. Fei and F. Huang, "New Visible Watermark Protection Mechanism Based on Information Hiding," in *IEEE Transactions on Information Forensics and Security*, vol. 20, pp. 7764-7776, 2025.
8. H. Wang, J. Fei, **Y. Dai**, L. Leng, Z. Xia. General GAN-Generated Image Detection by Data Augmentation in Fingerprint Domain. 2023 IEEE International Conference on Multimedia and Expo. IEEE, 2023: 1187-1192.
9. J. Chen, **Y. Dai** and F. Huang, DiffAttack: Imperceptible and Transferable Audio Adversarial Attack via Diffusion Model, 2025 IEEE International Conference on Acoustics, Speech and Signal Processing (ICASSP 2025), Hyderabad, India, IEEE, 2025, pp. 1-5.
10. J. Yang, Y. Wang, Y. Fang, **Y, Dai** and F. Huang, "Variance as a Catalyst: Efficient and Transferable Semantic Erasure Adversarial Attack for Customized Diffusion Models", In Proceedings of the 42th International Conference on Machine Learning (ICML 2025), Vancouver, Canada.

Awards

1. National Scholarship for Graduate Students, December 2022, Ministry of Education of the People's Republic of China
2. National Bronze Award, 8th China International College Students' "Internet+" Innovation and Entrepreneurship Competition, November 2022, Ministry of Education of the People's Republic of China (Team Leader)
3. National First Prize, 18th Huawei Cup China Postgraduate Mathematical Contest in Modeling, December 2021, China Society of Degree and Graduate Education