Hanzhou WU

Shanghai University
99 Shangda Road, Baoshan District
Shanghai 200444, China

h.wu.phd@ieee.org
alt: hanzhou@shu.edu.cn
https://hzwu.github.io

EDUCATION

Southwest Jiaotong University 2011 – 2017
Ph.D. in Information Security *Chengdu 611756, Sichuan, China*

Southwest Jiaotong University 2007 – 2011
B.Sc. in Information Security (with Mao Yisheng Honors Class) *Chengdu 611756, Sichuan, China*

PROFESSIONAL EXPERIENCE

Associate Professor 2021 –
School of Communication and Information Engineering, Shanghai University *Shanghai 200444, China*

Assistant Professor 2019 – 2021
School of Communication and Information Engineering, Shanghai University *Shanghai 200444, China*

Research Scientist 2017 – 2019
Institute of Automation, Chinese Academy of Sciences *Beijing 100190, China*

Visiting Scholar 2014 – 2016
Dept. of Electrical and Computer Engineering, New Jersey Institute of Technology *Newark 07102, NJ, USA*

TEACHING

Artificial Intelligence Foundation Spring
Deep learning, neural networks, large language models, conventional machine learning, etc.

Information Networks and Security Spring
Cryptography, firewall, intrusion detection, network security protocols, etc.

Matrix Theory and Methods Fall
Linear space, norms, spectral theory, matrix factorizations, generalized inverses, etc.

Computer Programming (C Language) Fall
pointer, array, queue, structure, tree, graph, file input and output, etc.

RESEARCH INTERESTS

Information Forensics and Security: *LLM security, AI security, multimedia security, multimedia forensics, multimedia signal processing, steganography/steganalysis, digital watermarking, etc.*

KEY WORDS OF RESEARCH

image/video/audio signal processing, natural language processing, information hiding, data hiding, digital watermarking, steganography, steganalysis, covert communication, deep learning, computer security, artificial intelligence, intellectual property protection, deep neural networks, backdooring, digital forensics, tamper detection and localization, quantum computing, language model, large language model, linguistic steganography, linguistic steganalysis, reversible data hiding, reversible watermarking, authentication, data embedding, graph neural networks, adversarial examples, ownership verification, data poisoning, quantum artificial intelligence, anomaly detection, machine learning, explainability, game theory, cryptography, network security, wireless communication, etc.

SELECTED MEDIA, AWARDS AND HONORS

Feature Interview: Watermarking the World of Data
Magazine "Scientific Chinese" *2025*

World's Top 2% Scientists https://topresearcherslist.com/
released by Stanford University *2025*

Outstanding Paper Award
co-author, in China Media Forensics and Security Workshop *2023*

CCF-Tencent Rhino-Bird Young Faculty Open Research Fund
Principal Investigator, supported by Tencent Inc. *2022*

Best Presentation Award
first author, in China Media Forensics and Security Workshop *2021*

Outstanding Paper Award
first author, in China Information Hiding and Multimedia Security Workshop *2019*

Shanghai "Chenguang" Program
Principal Investigator, supported by Shanghai Municipal Education Commission *2019*

Silver Medal
contestant, 36th ACM-ICPC Asia Regional Programming Contest (Chengdu Site) *2011*

Silver Medal
contestant, 36th ACM-ICPC Beijing Invitational Programming Contest *2011*

Silver Medal
contestant, "Google Cup" ACM-ICPC Fudan Invitational Programming Contest *2011*

Bronze Medal
contestant, 35th ACM-ICPC Asia Regional Programming Contest (Hangzhou Site) *2010*

Bronze Medal
contestant, 35th ACM-ICPC Asia Regional Programming Contest (Tianjin Site) *2010*

SELECTED ACTIVITIES AND SERVICES

Associate Editor
IEEE Signal Processing Letters *2025 –*

Editorial Board Member
Scientific Reports, Springer Nature *2025 –*

Technical Committee Member
APSIPA Multimedia Security and Forensics (MSF) *2023 –*

Steering Committee Member
14th – 18th International Conference on Advances in Multimedia *2022 – 2026*

Publicity Chair
8th International Conference on Frontiers in Cyber Security (Guiyang, China) *2025*

Special Session Organizer
13th International Conference on Communications and Broadband Networking (Chengdu, China) *2025*

Special Session Organizer
APSIPA Annual Summit and Conference (Macau, China) *2024*

Local Organization Chair
14th IEEE International Workshop on Information Forensics and Security (Shanghai, China) *2022*

Keynote Speech
14th International Conference on Advances in Multimedia (Barcelona, Spain) *2022*

Session Chair
IEEE International Symposium on Biometrics and Security Technologies (Chengdu, China) *2013*

Reviewer
for influential journals and conferences covering information forensics and security, e.g., IEEE SPL. *often*

FUNDING / SPONSORS (Total funding as of 12/31/2024: CNY 3,000,000+)

Nanning Science and Technology Bureau
Principal Investigator for Shanghai University, CNY 270,000 / 450,000 (60%) *2025 – 2028*

Science and Technology Department of Guizhou Province
Principal Investigator, CNY 200,000 *2025 – 2028*

Science and Technology Commission of Shanghai Municipality
Principal Investigator, CNY 200,000 *2024 – 2027*

National Natural Science Foundation of China
Principal Investigator for Shanghai University, CNY 768,000 / 2,560,000 (30%) *2024 – 2027*

Science and Technology Department of Tibet
Principal Investigator for Shanghai University, CNY 900,000 / 3,000,000 (30%) *2024 – 2026*

CCF-Tencent Rhino-Bird Young Faculty Open Research Fund
Principal Investigator, CNY 150,000 *2022 – 2023*

Shanghai "Chen Guang" Program
Principal Investigator, CNY 60,000 *2020 – 2022*

National Natural Science Foundation of China
Principal Investigator, CNY 280,000 *2020 – 2022*

China Scholarship Council
Principal Investigator, USD 40,800 *2014 – 2016*

BOOKS AND BOOK CHAPTERS

Elsevier'20 H. Wu. Unsupervised steganographer identification via clustering and outlier detection. In: *Digital Media Steganography (Chapter 13)*, Elsevier, 2020.

IOP Science'21 H. Wu. Recent advances in reversible watermarking in an encrypted domain. In: *Advanced Security Solutions for Multimedia (Chapter 4)*, IOP Science, 2021.

IntechOpen'21 H. Wu. Graph models in information hiding. In: *Recent Applications in Graph Theory (Chapter 1)*, IntechOpen, 2021.

Springer'24 H. Wu, T. Yang, X. Zheng, Y. Fang. Linguistic steganography and linguistic steganalysis. In: *Adversarial Multimedia Forensics (Chapter 7)*, Springer, 2024.

SELECTED JOURNAL ARTICLES

IEEE SPL'16 G. Xu, H. Wu, Y. Shi. Structural design of convolutional neural networks for steganalysis. *IEEE Signal Processing Letters*, vol. 23, no. 5, pp. 708-712, 2016.

IEEE TCSVT'17 H. Wu, Y. Shi, H. Wang, L. Zhou. Separable reversible data hiding for encrypted palette images with color partitioning and flipping verification. *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 27, no. 8, pp. 1620-1631, 2017.

IEEE TCSVT'20 F. Ding, H. Wu, G. Zhu, Y. Shi. METEOR: Measurable energy map toward the estimation of resampling rate via a convolutional neural network. *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 30, no. 12, pp. 4715-4727, 2020.

Elsevier SP'21 Y. Qin, H. Wu, G. Feng. Structured subspace learning-induced symmetric nonnegative matrix factorization. *Signal Processing*, vol. 186, p. 108115, 2021.

IEEE CIM'21 Z. Wang, G. Feng, H. Wu, X. Zhang. Data hiding in neural networks for multiple receivers. *IEEE Computational Intelligence Magazine*, vol. 16, no. 4, pp. 70-84, 2021.

IEEE TDSC'21 Y. Chen, H. Wang, H. Wu, Z. Wu, T. Li, A. Malik. Adaptive video data hiding through cost assignment and STCs. *IEEE Transactions on Dependable and Secure Computing*, vol. 18, no. 3, pp. 1320-1335, 2021.

IEEE SPL'21 H. Wu, B. Yi, F. Ding, G. Feng, X. Zhang. Linguistic steganalysis with graph neural networks. *IEEE Signal Processing Letters*, vol. 28, pp. 558-562, 2021.

IEEE TCSVT'21 H. Wu, G. Liu, Y. Yao, X. Zhang. Watermarking neural networks with watermarked images. *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 31, no. 7, pp. 2591-2601, 2021.

Elsevier PR'22 Y. Qin, H. Wu, J. Zhao, G. Feng. Enforced block diagonal subspace clustering with closed form solution. *Pattern Recognition*, vol. 130, p. 108791, 2022.

IEEE TIP'22 Y. Qin, H. Wu, X. Zhang, G. Feng. Semi-supervised structured subspace learning for multi-view clustering. *IEEE Transactions on Image Processing*, vol. 31, pp. 1-14, 2022.

IEEE CL'22 L. Zhou, C. Zhang, Q. Zeng, X. Liu, H. Wu. Optimal low-hit-zone frequency-hopping sequence sets with wide-gap for FHMA systems under follower jamming. *IEEE Communications Letters*, vol. 26, no. 5, pp. 969-973, 2022.

IEEE SPL'22 B. Yi, H. Wu, G. Feng, X. Zhang. ALiSa: Acrostic linguistic steganography based on BERT and Gibbs sampling. *IEEE Signal Processing Letters*, vol. 29, pp. 687-691, 2022.

Elsevier CS'23 T. Qiao, Y. Ma, N. Zheng, H. Wu, Y. Chen, M. Xu, X. Luo. A novel model watermarking for protecting generative adversarial network. *Computers & Security*, vol. 127, p. 103102, 2023.

Elsevier ESWA'23 J. Wang, D. Wu, L. Li, J. Zhao, H. Wu, Y. Tang. Robust periodic blind watermarking based on sub-block mapping and block encryption. *Expert Systems with Applications*, vol. 224, p. 119981, 2023.

IEEE SJ'23 L. Xiong, T. Peng, F. Li, S. Zeng, H. Wu. Privacy-preserving authentication scheme with revocability for multi-WSN in industrial IoT. *IEEE Systems Journal*, vol. 17, no. 1, pp. 38-49, 2023.

Elsevier PRL'23 H. Wu, C. Li, G. Liu, X. Zhang. Hiding data hiding. *Pattern Recognition Letters*, vol. 165, pp. 122-127, 2023.

IEEE TCSVT'23 S. Chen, A. Malik, X. Zhang, G. Feng, H. Wu. A fast method for robust video watermarking based on Zernike moments. *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 33, no. 12, pp. 7342-7353, 2023.

Elsevier InfoSci'24 Y. Liu, C. Li, Z. Wang, H. Wu, X. Zhang. Transferable adversarial attack based on sensitive perturbation analysis in frequency domain. *Information Sciences*, vol. 678, p. 120971, 2024.

IEEE TDSC'24 T. Yang, H. Wu, B. Yi, G. Feng, X. Zhang. Semantic-preserving linguistic steganography by pivot translation and semantic-aware bins coding. *IEEE Transactions on Dependable and Secure Computing*, vol. 21, no. 1, pp. 139-152, 2024.

IEEE TKDE'24 Y. Qin, N. Pu, H. Wu. Elastic multi-view subspace clustering with pairwise and high-order correlations. *IEEE Transactions on Knowledge and Data Engineering*, vol. 36, no. 2, pp. 556-568, 2024.

IEEE IoT'24 X. Zhao, H. Wu, X. Zhang. Effective backdoor attack on graph neural networks in spectral domain. *IEEE Internet of Things Journal*, vol. 11, no. 7, pp. 12102-12114, 2024.

IEEE TKDE'24 Y. Qin, Z. Tang, H. Wu, G. Feng. Flexible tensor learning for multi-view clustering with markov chain. *IEEE Transactions on Knowledge and Data Engineering*, vol. 36, no. 4, pp. 1552-1565, 2024.

IEEE TMM'24 Y. Qin, N. Pu, H. Wu. EDMC: Efficient multi-view clustering via cluster and instance space learning. *IEEE Transactions on Multimedia*, vol. 26, pp. 5273-5283, 2024.

IEEE IoT'24 Y. Liu, L. Zhang, H. Wu, Z. Wang, X. Zhang. Reducing high-frequency artifacts for generative model watermarking via wavelet transform. *IEEE Internet of Things Journal*, vol. 11, no. 10, pp. 18503-18515, 2024.

IEEE IoT'24 D. Wu, J. Wang, J. Zhao, L. Li, Z. Wang, H. Wu. Adaptive robust watermarking for resisting multiple distortions in real scenes. *IEEE Internet of Things Journal*, vol. 11, no. 10, pp. 33229-33246, 2024.

IEEE TCSVT'24 L. Lin, D. Wu, J. Wang, Y. Chen, X. Zhang, H. Wu. Automatic, robust and blind video watermarking resisting camera recording. *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 34, no. 12, pp. 13413-13426, 2024.

IEEE IoT'24 J. Wang, J. Zhao, L. Li, Z. Wang, H. Wu, D. Wu. Robust blind video watermarking based on ring tensor and BCH coding. *IEEE Internet of Things Journal*, vol. 11, no. 24, pp. 40743-40756, 2024.

IEEE TMM'25 Y. Qin, N. Pu, H. Wu, N. Sebe. Discriminative anchor learning for efficient multi-view clustering. *IEEE Transactions on Multimedia*, vol. 27, pp. 1386-1396, 2025.

ACM TKDD'25 Y. Qin, N. Pu, H. Wu, N. Sebe. Margin-aware noise-robust contrastive learning for partially view-aligned problem. *ACM Transactions on Knowledge Discovery from Data*, vol. 19, no. 1, pp. 1-20, 2025.

IEEE TCE'25 L. Xiong, J. Wang, L. Yu, N. Xiong, H. Wu. An efficient privacy-preserving access control scheme for cloud computing services. *IEEE Transactions on Consumer Electronics*, vol. 71, no. 2, pp. 6642-6658, 2025.

IEEE IoT'25 L. Li, X. Zhang, H. Wu, G. Feng, W. Zhang. FareMark: Model-watermark-driven free-rider detection in federated learning model. *IEEE Internet of Things Journal*, vol. 12, no. 18, pp. 38965-38977, 2025.

IEEE IoT'25 X. Ren, H. Wu, Y. Wang, H. Liu, X. Lu, G. Sun. StegGuard: Secrets encoder and decoder act as fingerprint of self-supervised pre-trained model. *IEEE Internet of Things Journal*, vol. 12, no. 18, pp. 38172-38184, 2025.

Elsevier InfoSci'26 W Yang, Y Liu, Y Chen, Y Cui, C Guo, G Shen, H Wu. HSMNet: A multi-resolution grayscale image steganalysis method based on hybrid dilated convolution and self-attention multi-channel network. *Information Sciences*, vol. 728, p. 122824, 2026.

Elsevier NN'26 J. Hu, L. Li, H. Wu, H. Luo, X. Zhang. Dormant key: unlocking universal adversarial control in text-to-image models. *Neural Networks*, vol. 193, p. 108065, 2026.

SELECTED CONFERENCE PAPERS

IH&MMSec'16 H. Wu, H. Wang, Y. Shi. PPE-based reversible data hiding. In: *Proc. ACM Workshop on Information Hiding and Multimedia Security*, pp. 187-188, 2016.

IH&MMSec'16 G. Xu, H. Wu, Y. Shi. Ensemble of CNNs for steganalysis: an empirical study. In: *Proc. ACM Workshop on Information Hiding and Multimedia Security*, pp. 103-107, 2016.

WIFS'16 H. Wu, H. Wang, Y. Shi. Dynamic content selection-and-prediction framework applied to reversible data hiding. In: *Proc. IEEE International Workshop on Information Forensics and Security*, pp. 1-6, 2016.

MWSF'19 H. Wu, W. Wang, J. Dong, H. Wang. New graph-theoretic approach to social steganography. In: *Proc. IS&T Electronic Imaging, Media Watermarking, Security and Forensics*, pp. 539-1-539-7, 2019.

MWSF'20 H. Wu, X. Zhang. Reducing invertible embedding distortion using graph matching model. In: *Proc. IS&T Electronic Imaging, Media Watermarking, Security and Forensics*, pp. 21-1-21-10, 2020.

MWSF'20 J. Wang, H. Wu, X. Zhang, Y. Yao. Watermarking in deep neural networks via error back-propagation. In: *Proc. IS&T Electronic Imaging, Media Watermarking, Security and Forensics*, pp. 22-1-22-9, 2020.

MWSF'20 H. Kang, H. Wu, X. Zhang. Generative text steganography based on LSTM network and attention mechanism with keywords. In: *Proc. IS&T Electronic Imaging, Media Watermarking, Security and Forensics*, pp. 291-1-291-8, 2020.

ICASSP'20 H. Wu. Patch-level selection and breadth-first prediction strategy for reversible data hiding. In: *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. 2837-2841, 2020.

WIFS'21 X. Zhao, Y. Yao, H. Wu, X. Zhang. Structural watermarking to deep neural networks via network channel pruning. In: *Proc. IEEE International Workshop on Information Forensics and Security*, pp. 1-6, 2021.

ICASSP'22 B. Yi, H. Wu, G. Feng, X. Zhang. Exploiting language model for efficient linguistic steganalysis. In: *Proc. IEEE International Conference on Acoustics, Speech, and Signal Processing*, pp. 3074-3078, 2022.

MWSF'24 H. Wu. Prompting steganography: a new paradigm. In: *Proc. IS&T Electronic Imaging, Media Watermarking, Security and Forensics*, pp. 338-1-338-11, 2024.

IH&MMSec'24 C. He, D. Wu, X. Zhang, H. Wu. Watermarking text documents with watermarked fonts. *ACM Workshop on Information Hiding and Multimedia Security*, pp. 187-197, 2024.

IH&MMSec'24 L. Zhang, Y. Liu, X. Zhang, H. Wu. Suppressing high-frequency artifacts for generative model watermarking by anti-aliasing. *ACM Workshop on Information Hiding and Multimedia Security*, pp. 223-234, 2024.

WIFS'24 X. Zhao, H. Wu, X. Zhang. Transferable watermarking to self-supervised pre-trained graph encoders by trigger embeddings. In: *Proc. IEEE International Workshop on Information Forensics and Security*, pp. 1-6, 2024.

MM'25 Y. Qin, N. Pu, H. Wu, Z. Fan. Flexible multi-view clustering with dynamic views generation. In: *Proc. ACM International Conference on Multimedia*, pp. 1072-1081, 2025.

MWSF'26 Z. Yang, H. Wu. A fingerprint for large language models. In: *Proc. IS&T Electronic Imaging, Media Watermarking, Security and Forensics*, to appear, 2026.

MWSF'26 H. Wu, Y. Wang. Defining cost function of steganography with large language models. In: *Proc. IS&T Electronic Imaging, Media Watermarking, Security and Forensics*, to appear, 2026.

MWSF'26 Y. Xu, G. Zhao, H. Wu, X. Zhang. Task migration resistant watermarking for natural language encoders. In: *Proc. IS&T Electronic Imaging, Media Watermarking, Security and Forensics*, to appear, 2026.

* Google Scholar: *https://scholar.google.com/citations?user=IdiF7M0AAAAJ&hl=en*

SELECTED SCHOLARS WHO CITED MY PUBLICATIONS

Geoffrey Hinton A.M. Turing Award Laureate, University of Toronto, Canada

Yoshua Bengio A.M. Turing Award Laureate, University of Montreal, Canada

Andrew Yao A.M. Turing Award Laureate, Tsinghua University, China

Jessica Fridrich Binghamton University, State University of New York, United States

Mauro Barni University of Siena, Italy

.....

* Last update: December 2025