

Hanzhou Wu

99 Shangda Road, Baoshan District
Shanghai 200444, China

h.wu.phd@ieee.org
<https://hzwu.github.io>

EDUCATION

Southwest Jiaotong University <i>Ph.D. in Information Security</i>	September 2011 – June 2017 <i>Chengdu 611756, Sichuan, China</i>
Southwest Jiaotong University <i>B.Sc. in Information Security (with Mao Yisheng Honors Class)</i>	September 2007 – June 2011 <i>Chengdu 611756, Sichuan, China</i>

PROFESSIONAL EXPERIENCE

Adjunct Professor <i>School of Big Data and Computer Science, Guizhou Normal University</i>	January 2024 – Present <i>Guiyang 550025, Guizhou, China</i>
Associate Professor <i>School of Communication and Information Engineering, Shanghai University</i>	March 2021 – Present <i>Shanghai 200444, China</i>
Assistant Professor <i>School of Communication and Information Engineering, Shanghai University</i>	March 2019 – February 2021 <i>Shanghai 200444, China</i>
Research Scientist <i>Institute of Automation, Chinese Academy of Sciences</i>	July 2017 – February 2019 <i>Beijing 100190, China</i>
Visiting Scholar <i>Dept. of Electrical and Computer Engineering, New Jersey Institute of Technology</i>	October 2014 – October 2016 <i>Newark 07102, NJ, USA</i>

TEACHING

-
- Matrix Theory and Methods (graduate course), Spring
 - Information Networks and Security (undergraduate course), Spring
 - C Language Programming (undergraduate course), Fall
 - Multimedia Security (undergraduate course), Fall

RESEARCH INTERESTS

digital watermarking, steganography, steganalysis, digital forensics and so on.

SELECTED AWARDS AND HONORS

Outstanding Paper Award <i>co-author, in China Media Forensics and Security Workshop</i>	November 2023
CCF-Tencent Rhino-Bird Young Faculty Open Research Fund <i>Principal Investigator, supported by Tencent Inc.</i>	August 2022
Best Presentation Award <i>first author, in China Media Forensics and Security Workshop</i>	November 2021
Outstanding Paper Award <i>first author, in China Information Hiding and Multimedia Security Workshop</i>	October 2019
Shanghai “Chengguang” Program <i>Principal Investigator, supported by Shanghai Municipal Education Commission</i>	December 2019
Silver Medal <i>contestant, 36th ACM-ICPC Asia Regional Programming Contest (Chengdu Site)</i>	November 2011

Silver Medal*contestant, 36th ACM-ICPC Beijing Invitational Programming Contest**June 2011***Silver Medal***contestant, “Google Cup” ACM-ICPC Fudan Invitational Programming Contest**May 2011***Bronze Medal***contestant, 35th ACM-ICPC Asia Regional Programming Contest (Hangzhou Site)**October 2010***Bronze Medal***contestant, 35th ACM-ICPC Asia Regional Programming Contest (Tianjin Site)**September 2010***SELECTED ACTIVITIES AND SERVICES**

Guest Editor*New Solutions for Multimedia and Artificial Intelligence Security, Mathematics**2024***Special Session Chair***“AI-Driven Innovations in Cybersecurity ...”**APSIPA Annual Summit and Conference (Macau, China)**2024***Student Program Chair***12th International Conference on Communications and Broadband Networking (Tibet, China)**2024***Technical Committee Member***IEEE International Conference on Computer Vision and Machine Intelligence (Allahabad, India)**2024***Steering Committee Member***16th International Conference on Advances in Multimedia (Barcelona, Spain)**2024***Technical Committee Member***APSIPA Multimedia Security and Forensics (MFS)**November 2023 - Present***Invited Speech***“Information hiding and its detection”**Binjiang Institute of Zhejiang University (Hangzhou, China)**2023***Invited Speech***“Multimedia and AI security”**Rhino-Bird Middle School Science Talents Training Program (Tencent Inc.)**2023***Invited Speech***“Interpretable model watermarking in frequency domain”**Shenzhen University (Shenzhen, China)**2023***Invited Speech***“Model watermarking for speech signal processing”**A2M Summit (Shanghai, China)**2023***Steering Committee Member***15th International Conference on Advances in Multimedia (Venice, Italy)**2023***Keynote Speaker***“Advances in DNN watermarking”**14th International Conference on Advances in Multimedia (Barcelona, Spain)**2022***Steering Committee Member***14th International Conference on Advances in Multimedia (Barcelona, Spain)**2022***Local Organization Chair***14th IEEE International Workshop on Information Forensics and Security (Shanghai, China)**2022***Lead Guest Editor***Advances in AI-related Information Forensics and Security, Security and Communication Networks**2022***Lead Guest Editor***Information Hiding - New Applications and Solutions, International Journal of Distributed Sensor Networks**2021*

FUNDINGS

Science and Technology Department of Tibet

Principal Investigator for Shanghai University, RMB 900,000/3,000,000

June 2024 - May 2026

National Natural Science Foundation of China

Principal Investigator for Shanghai University, RMB 768,000/2,560,000

January 2024 - December 2027

CCF-Tencent Rhino-Bird Young Faculty Open Research Fund

Principal Investigator, RMB 150,000

October 2022 - December 2023

Shanghai “Chen Guang” Program

Principal Investigator, RMB 60,000

January 2020 - December 2022

National Natural Science Foundation of China

Principal Investigator, RMB 280,000

January 2020 - December 2022

China Scholarship Council

Visiting Scholar, USD 40,800 + round-trip flight tickets

October 2014 - October 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 PUBLICATIONS

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.

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.

IEEE 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.

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 ICPR’18 H. Wu, W. Wang, J. Dong, H. Wang. Ensemble reversible data hiding. In: *Proc. IEEE International Conference on Pattern Recognition*, pp. 2676-2681, 2018.

- EI 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.
- EI 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.
- EI 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.
- EI 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.
- IEEE 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.
- 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.
- 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.
- IETE TR'21 H. Wu, X. Zhang. Game-theoretic analysis to parameterized reversible watermarking. *IETE Technical Review*, vol. 38, no. 1, pp. 26-35, 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.
- IEEE 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.
- 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.

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 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.

IEEE HPCC'22 H. Wu. Robust and lossless fingerprinting of deep neural networks via pooled membership inference. In: *Proc. IEEE International Conference on High Performance Computing and Communications*, pp. 1042-1049, 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.

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.

NeuCom'23 Z. Wang, G. Feng, H. Wu, X. Zhang. Data hiding during image processing using capsule networks. *Neurocomputing*, vol. 537, pp. 49-60, 2023.

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.

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.

NeuCom'23 M. Li, H. Wu, X. Zhang. A novel watermarking framework for intellectual property protection of NLG APIs. *Neurocomputing*, vol. 558, p. 126700, 2023.

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.

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.

EI 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.

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*, Early Access, 2024.
- IEEE TDSC'24 Y. Liu, H. Wu, X. Zhang. Robust and imperceptible black-box DNN watermarking based on Fourier perturbation analysis and frequency sensitivity clustering. *IEEE Transactions on Dependable and Secure Computing*, Early Access, 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.
- 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*, Early Access, 2024.
- 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 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*, Early Access, 2024.
- IEEE TMM'24 Y. Qin, N. Pu, H. Wu, N. Sebe. Discriminative anchor learning for efficient multi-view clustering. *IEEE Transactions on Multimedia*, Early Access, 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*, Early Access, 2024.

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

Last updated: August 2024