Isao Echizen, Professor, National Institute of Informatics (NII) (DL 2024-2025)

Title: Real or Fake? Frontiers of Countering Fake Media in the Age of Infodemics

Abstract: Gen AI can now learn from human-derived information such as the face, voice, body, and natural language to generate synthetic media that can be mistaken for the real thing. Synthetic media are used in a variety of applications in the fields of communication and entertainment. On the other hand, as a negative aspect of synthetic media, there are cases in which fake media, such as fake video, fake audio, and fake text, are generated and distributed for fraud, inducement of thought, and manipulation of public opinion. There is a fear of an "infodemic," a flood of uncertain information that causes anxiety and confusion in society. This talk will give an overview of the threats posed by such fake media and introduce the latest results of the national research project “Social Information Technologies to Counter Infodemics” (JST CREST FakeMedia) [1] and “SYNTHETIQ X: Research Platform for Defending and Preventing Spread of Fake Information” (JST K Program SYNTHETIQ X) [2] of the Japan Science and Technology Agency (JST).

[1] JST CREST FakeMedia, http://research.nii.ac.jp/~iechizen/crest-e.html

[2] JST K Program SYNTHETIQ X, https://research.nii.ac.jp/~iechizen/synthetiq-x/en/index.html

Bio: Isao Echizen is a director and a professor of the Information and Society Research Division, the National Institute of Informatics (NII), a director of the Global Research Center for Synthetic Media, the NII, and a professor in the Graduate School of Information Science and Technology, the University of Tokyo. He was a visiting professor at the University of Freiburg, Germany, and at the University of Halle-Wittenberg, Germany. He is currently engaged in research on multimedia security and multimedia forensics. He is a research director in the JST CREST FakeMedia project and in the JST K Program SYNTHETIQ X, Japan Science and Technology Agency (JST). He received the Commendation for Science and Technology by the Minister of Education, Culture, Sports, Science and Technology (Research category) and the IEICE Achievement Award in 2025, the IEEE Workshop on Information Forensics and Security Best Paper Award in 2017, the Information Security Cultural Award in 2016, and the DOCOMO Mobile Science Award in 2014. He is the Japanese representative on IFIP and on IFIP TC11 (Security and Privacy Protection in Information Processing Systems), a vice president of APSIPA. He is a fellow of IEICE, a fellow of IPSJ, and a senior member of IEEE.

Rohan Kumar Das, Research and Development (R & D) Manager at Fortemedia, Singapore division to lead the research and product development unit. (DL 2025-2026)

Title: Can We Still Trust the Voice?: Advancements in Deepfake Speech Detection

Abstract: Recent advancements in speech synthesis and voice conversion technology during the era of generative AI have enabled the creation of highly realistic deepfake speech, posing significant risks to security, privacy, and trust. This talk explores cutting-edge developments in speech deepfake detection, emphasizing both algorithmic innovations and practical applications. We will examine state-of-the-art approaches, including recent neural network architectures and acoustic feature analysis. Additionally, the talk will highlight various challenges in maintaining robustness against the evolving nature of speech deepfakes. By addressing these issues, this presentation provides insights into the current landscape of speech deepfake detection to outline future directions for research and deployment in safeguarding speech-based communication systems.

Bio: Rohan Kumar Das received Ph.D degree from Indian Institute of Technology (IIT) Guwahati in the year 2017. His Ph.D. work focused on speaker verification using short utterances from the perspective of practical application oriented systems. Prior to his research in the field of speech processing, he was a Project Scientist at Assam Science Technology and Environment Council from 2010 to 2011. After completing doctoral studies, he worked as a Data Scientist in Kovid Research Labs (now acquired by Kaliber Labs) and was involved in speech analytics based application services in 2017. Later that year, he joined Human Language Technology Laboratory, National University of Singapore as a Research Fellow and led the speaker verification group's research till March 2021. Currently, he is working as a Research and Development (R & D) Manager at Fortemedia, Singapore division to lead the research and product development unit. He was one of the organizers for special sessions on “The Attacker’s Perspective on Automatic Speaker Verification”, “Far-Field Speaker Verification Challenge 2020” in Interspeech 2020, the Voice Conversion Challenge 2020 and Face-voice Association in Multilingual Environments (FAME) Challenge 2024 in ACM Multimedia 2024. He has published over 100 research papers in peer reviewed journals and conferences. He is a Senior Member of IEEE, a member of ISCA and APSIPA.

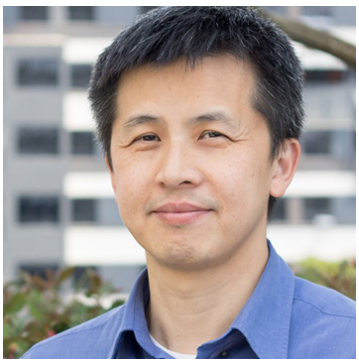
Xingri Li, Director of Product Engineering for High-Level Synthesis at Cadence Design Systems

Title: AI/ML-Powered High-Level Synthesis Solution

Abstract: This session introduces Stratus HLS, Cadence's high-level synthesis tool, designed to accelerate digital design productivity. Aimed at beginners, the presentation will cover the fundamentals of high-level synthesis and demonstrate how AI/ML technologies are being integrated into next-generation HLS solutions. Attendees will gain a foundational understanding of HLS and explore the innovative capabilities that Stratus HLS brings to modern SoC design.

Bio: Xingri Li is Director of Product Engineering for High-Level Synthesis at Cadence Design Systems. He specializes in digital design and verification methodologies and leads both the Solutions and Field Application Support teams across the Asia Pacific region. His focus is on developing product solutions and providing technical support for High-Level Synthesis customers. Before joining Cadence, Xingri spent seven years at Fujitsu Limited Japan as an SoC design engineer, where he worked on multimedia processing SoC chips. He also served as a principal engineer at Apical Imaging Limited for two years, specializing in advanced image processing implementations in FPGA and ASIC.
He holds a B.S. degree in Applied Physics from Nankai University, China (1998), and an M.S. degree in Informatics from Kyoto University, Japan (2002).

Ngai-Man (Man) Cheung, Associate Professor, Singapore University of Technology and Design (SUTD) (DL 2025-2026)



Title: Privacy Under Threat: Model Inversion in Deep Learning Systems

Abstract: Given a machine learning model trained on a private dataset, under what circumstances, and to what extent, can an adversary reconstruct private training samples by exploiting access to the trained model? This Model Inversion (MI) problem has significant privacy implications and could pose a critical threat to machine learning models. As these models are increasingly deployed in applications involving sensitive data—such as face recognition, automatic speaker recognition, medical diagnosis, and security—it is essential to understand the potential risks posed by the unauthorized reconstruction of private training samples. In this talk, I will discuss our work on studying MI attacks [1, 2], MI defenses [3], and MI-resilient architecture designs [4] to shed light on this critical privacy threat in modern deep neural networks.

[1] NB Nguyen, K Chandrasegaran, M Abdollahzadeh, NM Cheung. Re-thinking Model Inversion Attacks Against Deep Neural Networks. CVPR-2023.
[2] NB Nguyen, K Chandrasegaran, M Abdollahzadeh, NM Cheung. Label-Only Model Inversion Attacks via Knowledge Transfer. NeurIPS-2023.
[3] ST Ho, KJ Hao, K Chandrasegaran, NB Nguyen, NM Cheung. Model Inversion Robustness: Can Transfer Learning Help? CVPR-2024.
[4] JH Koh, ST Ho, NB Nguyen, NM Cheung. On the Vulnerability of Skip Connections to Model Inversion Attacks. ECCV-2024.

Bio: Ngai-Man (Man) Cheung is an Associate Pillar Head and Associate Professor with Singapore University of Technology and Design (SUTD). He receives his Ph.D. degree in Electrical Engineering from University of Southern California (USC), Los Angeles, CA. His Ph.D. research focused on image and video coding, and the work was supported in part by NASA-JPL. He was a postdoctoral researcher with the Image, Video and Multimedia Systems group at Stanford University, Stanford, CA. He was a core team member of the Foundational Research Capabilities Team for AI - National Research Foundation (NRF) Singapore, and an AI Advisor for Smart Nation and Digital Government ORice (SNDGO) in Singapore. His research has resulted in more than 200 papers and 14 U.S. patents granted with several pending. Two of his inventions have been licensed to companies. One of his research results has led to a SUTD spinoR on AI for healthcare. His research has also been featured in the National Artificial Intelligence Strategy. He has received several research recognitions, including the Best Paper Finalist at the IEEE Conference on Computer Vision and Pattern Recognition (CVPR) 2019, the Finalist of Super AI Leader (SAIL) Award at the World AI Conference (WAIC) 2019 at Shanghai, China. His research interests are Signal and Image Processing, Computer Vision and AI.

Minoru Kuribayashi, Professor, Tohoku University (DL 2025-2026)

Title: Ownership Verification of DNN Models

Abstract: With the advance of AI technologies, Machine Learning as a Service (MLaaS) platforms are emerging to facilitate transactions between model developers and end users. However, it has also given rise to significant challenges, particularly copyright infringement and ownership conflicts. To take countermeasures against misappropriation of trained models, DNN watermarking and fingerprinting have been investigated for the protection of intellectual property. The watermark/fingerprint reflects the behavior of the model on the given trigger images as the backdoor. The behavior is regarded as an identifier for the ownership verification. This talk will outline recent research on such ownership verification tasks. The potential, limitations, and future directions of this research will also be discussed.

Bio: Minoru Kuribayashi received B.E., M.E., and D.E degrees from Kobe University, Japan, in 1999, 2001, and 2004. He was a Research Associate and an Assistant Professor at Kobe University from 2002 to 2007 and from 2007 to 2015, respectively. He was an Associate Professor in the Graduate School of Natural Science and Technology, Okayama University from 2015 to 2023. Since 2023, he has been a Professor in Center for Data-driven Science and Artificial Intelligence at Tohoku University. His research interests include multimedia security, digital watermarking, cryptography, and coding theory. He served as an associate editor of IEEE Signal Processing Letters and Journal of Information Security and Applications, and IEICE. He was a TC member of IEEE SPS Information Forensics and Security. He was a chair of APSIPA TC of Multimedia Security and Forensics. He received the Young Professionals Award from IEEE Kansai Section in 2014, and the Best Paper Award from IWDW 2015 and 2019. He is a fellow of IEICE and senior member of IEEE.

Corey Manders

AI specialist, CTO of FAIT Pte. Ltd.

Title: FAIT (Financial AI Technology) using AI to connect enterprise systems

Abstract: For decades, organizations have relied on teams of Business Analysts and programmers to map data from one enterprise system to another. However, the process is slow, extremely expensive, and results in huge delays in the use and onboarding of new systems. The founders of FAIT realized this, and began creating a platform that would leverage LLMs to do much of the work that is needed to accomplish this mapping task. When using large teams to accomplish the mapping task, some aspects of what get left out are the ability to react to changes in mapping over time, and the ability to audit the data lineage at any point in time. The FAIT system creates mappings with this in mind. All of the mapping, build, and runtime tools employ well designed User Interfaces that are specifically designed to provide intuitive workflows for the users, while simultaneously using state-of-the-art LLMs in the backend to accomplish the mapping goals. The talk will demonstrate a few simple to complex mappings using the FAIT platform.

Bio: Research and development team leader in Artificial Intelligence, Machine Learning, AR/VR, and software development. Research scientist with substantial publications. Developed several programs dedicated to the capture and processing of digital images. Experienced lecturer on computer programming, engineering, and computational vision. Specialties: AR/VR, Tensorflow, Keras, ML, AI, Programming in several languages (Python, C/C++/C#, Java), image processing algorithms, machine learning, extended dynamic range imaging.