Title:

Adversarial Artificial Intelligence.

Abstract:

Due to the rapid development of technology, artificial intelligence technologies has demonstrated tremendous success in various tasks, such as computer vision, natural language processing, data mining, etc. Currently, the artificial intelligence technologies, which are dominated by the deep learning, may also encounter various security problems, such as model vulnerability-based attacks, data forgeries, illegal model distributions, etc., in practical adversarial environments. These problems tend to seriously interfere/degrade the performances of artificial intelligence methods, or deceive others, which may cause potential damages to the society and individuals.
In this workshop, we intend to attract the attentions from various research directions, such as adversarial attack and defence, data forgery and forensics, robust AI model, AI model protection, etc., to discuss the recent progresses and future directions in adversarial artificial intelligence.

Scope and Topics:

Potential topics include but are not limited to:

- ✧ Adversarial Attack
- ✧ Adversarial Defence
- ✧ Data Forgery Detection
- ✧ Data Forgery Localization
- ✧ Data Forgery Generation
- ✧ Backdoor Learning
- ✧ Robust AI Model
- ✧ Copyright Protection for AI Models

Program Committee Chairs:

Yuanfang GUO, Beihang University, China
Email: andyguo@buaa.edu.cn
Homepage: http://irip.buaa.edu.cn/andyguo/index.html
Bio: Yuanfang Guo received his B.Eng. degree in computer engineering and Ph.D. degree in electronic and computer engineering from the Hong Kong University of Science and Technology, Hong Kong, in 2009 and 2015, respectively. Then he served as an assistant professor with the State Key Laboratory of Information Security, Institute of Information Engineering, Chinese Academy of Sciences for three years. He is currently an Assistant Professor with the Laboratory of Intelligent Recognition and Image Processing, School of Computer Science and Engineering, Beihang

University, Beijing, China. His main research interests include multimedia security, artificial intelligence security, graph neural networks, and he has published over 60 scientific papers.
He is a senior member of the IEEE. He is currently serving as an associate editor of IET Image Processing and a senior PC member of IJCAI 2021. He has served as an area chair of ACM MM 2020. He has served as a PC member for multiple conferences including AAAI, IJCAI, ACM MM, etc., and was recognized as a distinguished PC member in IJCAI 2018. He has served as a reviewer for 10+ journals including IEEE TIP, IEEE TIFS, IEEE TCSVT, IEEE TMM, etc., and multiple conferences including NIPS, IEEE CVPR, IEEE ICCV, ECCV, etc., and was recognized as a distinguished reviewer in ICME 2020.

Sheng LI, Fudan University, China
Email: lisheng@fudan.edu.cn
Homepage: https://blazelisheng.github.io/
Bio: Sheng Li is currently an Associate Professor with the School of Computer Science, Fudan University, China. His research interests include biometric template protection, pattern recognition, multimedia forensics and security. He is the recipient of the IEEE WIFS Best Student Paper Silver Award.

Changsheng CHEN, Shenzhen University, China
Email: cschen@szu.edu.cn
Homepage: https://ceie.szu.edu.cn/info/1287/2383.htm
Bio: Changsheng Chen received the B.Eng. degree in software engineering from Sun Yat-sen University, Guangzhou, China in 2008 and the Ph.D. degree in Electrical and Electronic Engineering from Nanyang Technology University, Singapore in 2013. From 2013 to 2015, he worked as a PostDoc research associate at the HKUST Barcode Group, Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology. Since 2016, he has been with the Guangdong Key Laboratory of Intelligent Information Processing and Shenzhen Key Laboratory of Media Security, College of Electronics & Information Engineering, Shenzhen University, Shenzhen, China, where he is currently an Associate Professor. Dr. Chen's current research interests include 2D barcode, pattern recognition, machine learning and information security. He received the first prize from the world final of Inno-China Entrepreneurship Competition 2015. He serves as a Reviewer for the IEEE Transactions on Image Processing, the IEEE Transactions on Signal Processing, the IEEE Transactions on Information Forensics and Security, the IEEE Transactions on Multimedia, and so on.

Jiantao ZHOU, Macau University, Macau, China
Email: jtzhou@umac.mo
Homepage: https://www.fst.um.edu.mo/people/jtzhou/
Bio: Jiantao Zhou received the B.Eng. degree from the Department of Electronic Engineering, Dalian University of Technology, in 2002, the M.Phil. degree from the Department of Radio

Engineering, Southeast University, in 2005, and the Ph.D. degree from the Department of Electronic and Computer Engineering, Hong Kong University of Science and Technology, in 2009. He held various research positions at the University of Illinois at Urbana–Champaign, Hong Kong University of Science and Technology, and McMaster University. He is currently an Associate Professor with the Department of Computer and Information Science, Faculty of Science and Technology, University of Macau, and also the Interim Head of the newly established Centre for Artificial Intelligence and Robotics. He is also with the State Key Laboratory of Internet of Things for Smart City, and also with the Department of Computer and Information Science, University of Macau. His research interests include multimedia security and forensics, multimedia signal processing, artificial intelligence, and big data. He holds four granted U.S. patents and two granted Chinese patents. He has coauthored two articles that received the Best Paper Award at the IEEE Pacific-Rim Conference on Multimedia in 2007 and the Best Student Paper Award at the IEEE International Conference on Multimedia and Expo in 2016. He is an Associate Editor of the IEEE TRANSACTIONS ON IMAGE PROCESSING.

Program Committee:

Haodong LI, Shenzhen University, China
Xuping HUANG, AIIT, Japan
Ruijie YANG, Beihang University, China
Li DONG, Ningbo University, China
Ruikui WANG, Beihang University, China
Rui WANG, Institute of Information Engineering, Chinese Academy of Sciences, China
Yuanman LI, Shenzhen University, China
Hongyu YANG, Beihang University, China