**Graduate School of Information Science, University of Hyogo**
**7th International Research Seminar**

# SECURITY OF AI: IMAGE ANALYSIS FOCUS

Wed. 6 Nov. 2024 (16:00 ~ 17:00) JST

## ONLINE SEMINAR

The rapid advancements in artificial intelligence (AI) for image analysis have transformed industries like healthcare, security, autonomous driving, and social media. Yet, these advancements come with significant security challenges that we must urgently address. In this talk, we will delve into the complex security issues surrounding AI-driven image analysis, focusing on both recent developments and emerging threats. To begin, we'll explore different topics such as adversarial attacks, data poisoning, evasion attacks. Our discussion will include strategies to defend against these threats. Finally, we'll talk about the crucial role of regulatory frameworks and industry standards in ensuring the safe deployment of AI technologies. This talk aims to provide a thorough overview of the current landscape of AI security in image analysis, highlighting recent research, practical implications, and future directions.

## Guest Speaker

**Tarek Gaber**
Senior Lecturer,
University of Salford, UK

University of Salford
MANCHESTER

Tarek Gaber is a Senior Lecturer at the University of Salford, UK, & a Full Professor at Suez Canal University, Egypt. Dr. Gaber received his PhD in Computer Science (information security) from the University of Manchester in 2012. He has worked in many universities including the Faculty of Computers and Informatics, Suez Canal University, Faculty of Computers and Information Sciences, Ain Shams University, and the School of Computer Science, University of Manchester, Manchester, UK. He had a postdoctoral position at the Faculty of Electrical Engineering and Computer Science, VSB Technical University of Ostrava, Ostrava, Czech Republic. He is also a member of The Scientific Research Group in Egypt (SRGE). He has served as a co-chair and PC member in many international conferences and reviewed many scientific papers and participated in many scientific events (national/international conferences and workshops). He also served as Lead Guest Editor in many SCI international journals, including Applied Sciences, Wireless Communications and Mobile Computing, Sustainability, and Electronics. He has more than 100 publications in international journals, conferences, and book chapters. In addition, Dr. Gaber has published 5 edited books and served as a keynote speaker at many international conferences. Tarek has successfully supervised many MSc-by-Research students and PhD students. His major research interests include Cyber Security, Machine Learning, Artificial Intelligence, Secure Software Engineering.

## Register here (free)

https://shorturl.at/W2AOU

Contact: rashed@gsis.u-hyogo.ac.jp

## For more details:

https://shorturl.at/KhNx0