UNIVERSITY AT ALBANY
State University of New York

College of Arts and Sciences
Department of Mathematics and Statistics

Applied Topology in Albany (ATiA) Seminar

Ming-Ching Chang
SUNY Albany

Trustworthy AI in a Smarter World: Addressing Awareness, Authenticity, and Security Challenges

Friday, April 10, 2026
12:00 p.m. Hudson 0110

Abstract. Trustworthy AI research aims to create AI models that are efficient, robust, secure, fair, privacy-preserving, and accountable. As the adoption of Foundation Models and Generative AI grows, enabling the composition of articles and the generation of hyper-realistic images, the boundary between authenticity and deception is increasingly blurred in our rapidly evolving digital landscape. The demand for sophisticated tools and techniques to authenticate media content and discern the real from the fake has never been more urgent.

In this talk, I will explore recent breakthroughs in Trustworthy AI, Digital Media Forensics, and secure computation. First, I will introduce a novel approach to learning multi-manifold embeddings for Out-of-Distribution (OOD) detection, along with a method for uncovering hidden hallucination factors in large vision-language models through causal analysis. Additionally, I will cover a noisy-label learning technique designed to tackle long-tailed data distributions.

In the field of Digital Media Forensics, I will showcase novel advancements in Image Manipulation Detection (IMD) using implicit neural representations under limited supervision. This includes the development of IMD datasets featuring object-awareness and semantically significant annotations, leveraging stable diffusion to emulate real-world scenarios more effectively.

Finally, if time allows, I will cover recent works in secure encrypted computation, particularly in accelerating Fully Homomorphic Encryption (FHE) for deep neural network inference using GPUs, as well as enhancing functional bootstrapping through quantization and network fine-tuning strategies.