Title: Deceptive Media Manipulation – An arms race: Learning to defend & deceive

Abstract:

As digital manipulation techniques get better, it is becoming increasingly difficult to distinguish between real and fake data. Being able to model the real world and generate realistic data has many exciting applications. However, it poses a serious challenge when such data is generated by malicious actors with an intent to deceive the user (or the computer system) into believing that the fake data being generated is real. While such attacks on images have garnered much attention, they span across media types including speech & audio, text and, finally, fake news. To counter these attacks, intensive efforts have been undertaken by the ML community to generate effective defense strategies which malicious adversaries, in turn, seek to circumvent. This has led to a virtual arms race.

In this talk, I will provide an overview of the recent efforts in my group at Verisk. We have focused on developing algorithms to defend against expert manipulation of images as well as adversarial attacks that can bypass such defenses. Most of this work is hot off the press and under review at various conferences.

Bio:

Dr. Singh is Head R&D, Verisk | AI and the Director of the Human and Computation Intelligence Lab. His lab is working on creating collaborative (HMC, MMC) systems for efficient extraction of information & knowledge from unstructured data, capable of closed-loop & explainable reasoning and continuous learning, with applications in vision, NLP, speech and fintech.

Verisk Analytics delivers data analytic tools and services for risk assessment, risk forecasting and decision analytics in a variety of sectors including insurance, financial services, energy, government and human resources.

Dr. Singh has over 15 years of customer-focused industrial R&D experience with stints at Siemens CT and SRI International building and delivering image and video analytics technologies in the areas of multi-camera security and surveillance, aerial surveillance, advanced driver assistance and intelligent traffic control; industrial inspection; and, medical image processing and patient diagnostics systems. Dr. Singh received his Ph.D. in Electrical and Computer Engineering from the University of Illinois at in 2003. He has authored over 35 publications (1 best paper award), and has 15+ U.S. and International patents.