Report on Expert Talk Series

IEEE Computational Intelligence Society Chapter - IEEE Gujarat Section and Ahmedabad University organised second talk under its expert talk series with details as follows.

Title: Adversarial Examples of Deep Learning System and Its Defense

Speaker:  Professor Minoru Kuribayashi, Associate Professor, Okayama University, Japan

Mode: Virtual

Date: 15.03.2021

Time: 1100 am to 12.00 pm

Participants: About 110 under graduate students, PhD scholars, faculty members from Gujarat participated in the talk.

Abstract:  Deep neural network (DNN) is known to be vulnerable to adversarial attacks, where adversarial noise is added to images or speech files so that a target DNN-based system outputs wrong results. Adversarial examples are the content which fools a system. Examples of systems that can be attacked using adversarial examples include face recognition and automatic driving system. Moreover, the DNN training data set could also be poisoned in the situation where the adversary has access to the training database. One of the defense techniques is to detect such adversarial images by observing the outputs of a DNN-based system when noise removal filters are operated. Such operation-oriented characteristics enable us to classify a given image whether it is normal or adversarial. In this talk, I will show state-of-the-art techniques for detecting adversarial examples.

About Speaker:

 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. Since 2015, he has been an Associate Professor in the Graduate School of Natural Science and Technology, Okayama University. His research interests include multimedia security, digital watermarking, cryptography, and coding theory. He serves as an associate editor of JISA and IEICE. He is a vice chair of APSIPA TC of Multimedia Security and Forensics, and a TC member of IEEE SPS Information Forensics and Security. 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 senior member of IEEE and IEICE.