$1 Million Grant to Help Advance Machine Vision-Learning Technology

The award is aimed at teaching computers to detect, understand and build a defense capability against adversarial attacks.

BY ZENAIDA GONZALEZ KOTALA
AUGUST 13, 2020

Engineering Professor Mubarak Shah was recently awarded a $1 million grant to advance his cutting-edge work in the area of machine vision learning (artificial intelligence) and develop a system to thwart attacks on such systems.

Shah, the director of UCF’s Center for Research in Computer Vision, and his team work on a variety of research-teaching machines to detect objects and classify them, and to track objects in video and analyze their behavior. The research and technology the center develops has applications in an array of areas critical to the nation from scanning crowd scenes to detect and prevent threats, to analyzing brain scans for tumors.

For example, researchers from the center performed the first automated mass-crowd count. They were also able to use machine-learning techniques to develop a facial-recognition tool that promises to be useful in rapidly matching pictures of children with their biological parents and in potentially identifying photos of missing children as they age. In addition, they have developed a method to detect abnormal behavior in large crowds in an effort to help keep people safe from terrorist attacks. On the medical side, the center is using AI techniques to spot lung cancer from CT scans.

The new Department of Defense award is aimed at teaching computers to detect, understand and build a defense capability against adversarial attacks, which are carried out by mixed signals embedded in images that try to dramatically change the output decisions of Deep Neural Networks.

“We will develop techniques for generating universal adversarial perturbations that misclassify any input image of a given class to any other incorrectly. These attacks will be used as a mechanism to develop a mathematical framework to understand the underlying core principles of DNNs, attacks and defensive techniques, and to make the attack more robust to future defenses,” Shah says.

Shah will lead a team with electrical engineering Associate Professor Nazanin Rahnavaard. The team also includes graduate students and post-doctoral scholars, and long-time collaborator Professor Ajmal Mian at the University of Western Australia.

Shah, is the founding director of the Center for Research in Computer Vision at UCF. His research areas include video surveillance, visual tracking, human-activity recognition, visual analysis of crowded scenes, video registration and UAV video analysis. Shah is a fellow of IEEE, AAAS, IAPR and SPIE and was recently inducted into the National Academy of Inventors. In 2006, he was awarded a Pegasus Professor award, the highest faculty award at UCF. He has published dozens of papers and has more than 55,000 citations.