Intelligence Community Seeks AI Face Recognition Breakthrough in Competition

Officials see major improvement opportunities in fusing AI algorithms

Kevin McCaney

Wed, 07/11/2018 - 22:21

The intelligence community's research arm is looking to take face recognition technology to a new level with a fusion approach that could improve the identification of persons of interest while also making face recognition more reliable as an authentication tool.

The Intelligence Advanced Research Projects Activity, with help from the National Institute of Standards and Technology, is inviting industry and academia to take part in the Fusion of Face Recognition Algorithms 2018 Prize Challenge, in which participants will try to get more information out of a single image by using, and fusing, multiple algorithms.

“Face recognition has made significant advances in recent years and the fusion of more than one algorithm has shown to improve its accuracy,” IARPA program manager Chris Boehnen said in announcing the contest. “These fusion schemes could allow users to leverage multiple algorithms without overhauling or re-designing the core technologies.”

The technology IARPA hopes to generate through the contest would have across-the-board use in face recognition, though it wouldn’t necessarily apply to every scenario.

“The improvements sought within FOFRA would be relevant to watch list style recognition typical for a terrorism use case and to authentication verification scenarios such as securing a mobile device,” Boehnen said via email. “However, as fusion methods inherently have a higher computational cost (you're running more than one algorithm), it may not be the optimal choice if you are in a hardware constrained application with limited processing power,” he said. “From a practical perspective it would likely be applicable to most authentication scenarios, but there may be some applications when an extremely fast response is desired where it would be impractical.”

Image Isn’t Always Everything

Face recognition technology has come a long way in recent years. It’s used in multifactor biometric authentication systems for building and network access; as a way to scan crowds, passenger lists or criminal databases; and increasingly as the way to access smartphones. It’s also being tested as a way to confirm passengers on public transportation and validate financial transactions.

The Army Research Laboratory also has developed a system that does face recognition in the dark, using a thermal camera, an artificial intelligence and a machine learning technique to create a facial image in low-light situations.

But face recognition is far from perfect. Hackers and researchers have shown that some facial recognition apps can be fooled with 3D printed masks or augmented photos pulled from Facebook or other social media sites. And research has demonstrated how flaws in face recognition can result in law enforcement unfairly targeting innocent people. Every face can tell a story, but not all stories are complete, nor are they necessarily true.

Refining the Features

IARPA wants to take a good bit of uncertainty out of the process by expanding what face recognition can do. The agency already has its Janus program, which funds research into ways to fuse information from multiple views captured by "media in the wild," where people are always posting pictures of themselves and others. Rather than relying on posed, formally lit frontal images (license photos, mug shots), Janus would incorporate views from many angles, and use automated machine learning to process the data.

Current biometric fusion systems, which usually rely on artificial intelligence and deep learning systems, mostly combine two biometric modes, such as face and voice, iris and face, or face and fingerprint. IARPA and NIST want to stay within facial recognition, while "fusing the outputs of multiple face recognition algorithms applied to the same input images," according to NIST's description of the challenge.

IARPA notes that current face recognition systems have notable error rates, particularly with "uncontrolled face imagery," which could include, say, a blurred image from a surveillance camera or a partially hidden face, as opposed to a straight-ahead photo from a driver's license. Academic literature on biometric fusion describes significant gains that can be made by using more than one mode or algorithm. However, "The vast majority of the literature addresses biometric verification, rather than identification," IARPA says. Focusing on features rather than scores (such as the minutiae points on a fingerprint) could increase accuracy.

IARPA will supply the images and data, and NIST will test the submissions. In all, IARPA will award $70,000 in prizes across categories covering template and score-level fusion applied to verification and identification. Additional prizes will be awarded to entries that open-source their approaches. Registration for the challenge closes on Aug. 6.

View printer friendly version
Artificial Intelligence
NIST
IARPA
Intelligence Community