New possibilities for biometrics

May 31, 2018

Spartan researchers help create smarter, safer applications for a connected world

Every time you use your fingerprint to unlock your smartphone or access a banking app, you’re using biometrics—a way to authenticate identity using a unique biological characteristic.

Biometrics is becoming an increasingly common, and critical, component of our daily lives, and some of the nation’s foremost biometrics researchers at Michigan State University are leading exploration into applications that could make lives better by detecting health issues, preventing identity theft and enhancing security.

A core group of MSU researchers is using the power of algorithms and computations to conduct pioneering work in areas such as eye movement and face, iris and fingerprint recognition applications.

“MSU is a leader in biometrics academic research as well as the human capital that is trained here,” says Leo Kempel, dean of the College of Engineering. “We educate students who can go elsewhere and be leaders themselves.”

In addition to attracting and producing top talent, collaboration and real-world applications also contribute to MSU’s biometrics research success.

“What MSU has been very good at is interacting with industry, interacting with federal agencies, interacting with private enterprises and understanding what are the problems being faced in operational systems,” says Arun Ross, professor of computer science and engineering.
See some of the ways MSU is advancing the science of biometrics and creating solutions to the problems of today—and tomorrow.

LINKING IMPORTANT INFORMATION TO FINGERPRINTS

For more than 100 years, fingerprints have been used for personal identification. While early applications were limited to law enforcement and forensics, automated fingerprint identification systems are now used in a variety of settings, from unlocking personal devices to securing national borders.

Over the past 25 years, MSU researcher Anil Jain’s seminal contributions have pushed the frontiers of biometrics—in particular, fingerprint recognition. A University Distinguished Professor, Jain is widely regarded as one of the world’s top biometrics researchers and holds six U.S. patents on fingerprint recognition, as well as a host of accolades. His work has generated a wealth of knowledge that has inspired a generation of biometrics researchers and practitioners in academia and industry.

“MSU has a lineage of work in biometrics,” Jain says. “When people want to hire someone in biometrics, they look at our lab first.”

Jain has worked on the security and privacy of fingerprint recognition systems by creating and evaluating spoof fingers, tracking fingerprints of infants to help save lives and assisting police agencies in solving crimes.

His current work, with Ph.D. student Josh Engelsma, centers on the ability to track fingerprints of individuals and infants for health care monitoring and welfare distributions in even the most remote places in the world. Called Match in Box, the portable, high-resolution fingerprint recognition kit features easy-to-use, cost-effective technology that requires a simple touch of a finger. Once the fingerprint is collected, it is stored in the box and linked to a person’s identity and health records. With this information, Match in Box can help with vaccination tracking, health care and food and benefits distribution programs.

Match in Box is intentionally open source, meaning the technology, set-up and off-the-shelf hardware components are all made public, so people everywhere have the tools to make their own low-cost Match in Box.

“We are providing tools for everyone to build [fingerprint] readers, and to get the mystery out of it,” Jain says.
PREVENTING SPOOF ATTACKS AND SECURITY BREACHES

Thanks to the iPhone X, facial recognition—the ability to detect someone's identity based on facial characteristics—has become widespread.

At MSU, Xiaoming Liu, assistant professor of computer science and engineering, is looking for ways to prevent recreating people’s faces in order to assume their identity or access private information. It’s called face anti-spoofing.

“Face anti-spoofing aims to classify between real human faces and spoof attacks, such as a printed paper with faces, a cellphone playing face videos and a 3-D mask, based on the image or video input,” Liu says.

A big part of the biometrics work being done at MSU focuses on ways to intercept spoofing or recreation methods by those intending to use information nefariously.

To prevent a spoof, researchers must test various methods against their technology. Liu’s lab is doing just that with a new framework, or algorithm, they’ve created.

“We recently proposed a novel framework to face anti-spoofing that leverages auxiliary supervision,” he says, referring to additional ways to test against face spoofing, including depth of faces and how the nose protrudes out farther than cheeks. “Our framework is the best of its kind out there.”

In addition to facial recognition, there are many ongoing research projects on related computer vision problems, one of which is called monocular pedestrian detection.

Liu and Ph.D. student Garrick Brazil have developed technology that can detect when a person is present on or close to the road—such as in a bike lane or on the sidewalk. The hope is that this technology can one day be used in autonomous vehicles so a simple camera could be equipped to determine if a person is present.

“Since last year, for this capability we are actually the best among competitors on the benchmark evaluation, including
New possibilities for biometrics
Published on College of Engineering, Michigan State University (https://www.egr.msu.edu)

Microsoft, the University of California, San Diego and Facebook,” Liu says.

PROTECTING EYES AND IDENTITIES

While Liu’s research focuses on facial recognition, Ross is looking specifically at the iris of the eye, which surrounds the pupil. His research aims to prevent people from duplicating the iris of another person or modifying their own irises in order to fool a biometric system.

A project in Ross’s Integrated Pattern Recognition and Biometrics Lab, called Presentation Attack Detection, aims to detect various types of biometric replicas an adversary may use, including fake eyeballs, cosmetic contact lenses or photos of an iris.

To detect a fake or modified iris, Ross and his team have developed a powerful algorithm that takes a more nuanced look at the fidelity of an iris. This system successfully detects many types of fake attacks at nearly 100 percent accuracy.

This kind of research could help prevent unauthorized access to smartphones or bank accounts or catch people who are trying to circumvent a biometric watch list—ensuring new possibilities come with built-in safeguards.

TRACKING EYE MOVEMENT TO ASSESS OVERALL HEALTH

Tracking eye movements is a promising field within biometrics that enables researchers to derive internal information about individuals, particularly related to the eye muscles’ structure and brain function, says Oleg Komogortsev, associate professor of computer science and engineering, and the newest researcher in MSU’s biometrics group.

To help extract this information, Komogortsev is developing new cost- and power-effective infrared sensors, which, when included in a virtual reality, or VR, device, will be able to track eye movement with exceptionally high quality. And this kind of biometrics is extremely spoof-resistant.
Rather than using costly, image-based eye tracking technology, Komogortsev’s sensors will use only infrared light emitters and receivers driven by neural networks. After an individual uses a VR viewer equipped with the infrared sensor, the device could detect when something is amiss as it relates to the eyes or brain, thus enabling a health assessment application of the technology.

This research, funded by Google, the National Science Foundation and National Institute of Standards and Technology, may have such applications as interaction in VR using eye gaze, user authentication, health assessment and emotion detection, among others.

Komogortsev predicts in three to four years, the eye movement sensors developed in his lab will aid in detection of concussions, dementia, autism and other conditions that affect vision and cognition.

*Story written by Jennifer Orlando and courtesy of MSUToday.*