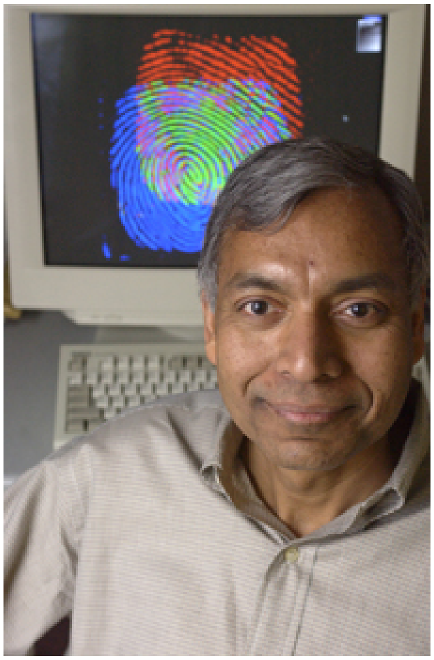
Biometric science seeks to avert identity crisis

February 20 2006



Anil Jain

Two things are certain about biometrics: It is the hot buzzword in identity management for convenience and protection from terrorists and identity thieves – and it's not foolproof.

Anil Jain, a University Distinguished Professor of computer science and engineering at Michigan State University, says the wizardry world of identifying people by unique physical characteristics -- fingerprints, the landscape of the iris, the digitized appearance and structure of their faces – is filled with promise.

But science still has work to do to deliver technology that meets the demands brought by threats of terrorism and identity theft.

"The advantages of biometrics is that it is based on who you are as opposed to what you have and what you know, such as ID cards or passwords," Jain said. "Biometrics is not necessarily proposed to replace the existing methods of identification, but to strengthen them. Having said that, there always are practical problems in deployment."

Jain told the American Association for the Advancement of Science annual meeting session on "Strengthening the Scientific Basis of Biometric Identification and Authentication" that science is developing better sensors to gather the data that pinpoint an individual's identity, and that science also has an opportunity to manage expectations and improve accuracy rates.

Biometrics has leaped from the world of fingerprinting criminals on blotters to enter the world of hi-tech scanners which are popping up at airports and grocery store cash registers. And it's not just fingers – the iris of the eye also holds unique, and highly accurate, identifying traits. Even faces – susceptible as they can be to age, weight and fashion – are succumbing to the algorithms and data fusion that science offers.

The precision of biometrics is impressive. While the performance depends on the testing protocol and environmental conditions, it can exceed 99 percent accuracy. Yet Jain notes that as the technology becomes more pervasive, even small margins of errors can have consequences that range from inconvenient and embarrassing to tragic.

One highly publicized example is the case of Brandon Mayfield, a

Portland, Ore., U.S. citizen held for two weeks as a suspect in the Madrid train bombings in 2004. The FBI fingerprint system matched prints at the scene to Mayfield, and an independent examiner verified the match. But Spanish National Police examiners eventually identified another man who matched the prints.

The FBI acknowledged the error and Mayfield was released.

Jain identified four areas of scientific emphasis:

-- Building better sensors. Jain noted that many of the problems with biometrics come because the scans are noisy and distorted. Fingerprints, for example, can be smudged or hard to read. Even new digital readers have downfalls. The act of pressing a finger to a glass plate can leave a residue that can be copied, allowing a fake finger to be made that can become a key to access. Jain said already better sensors are being developed that can differentiate between a live finger and a fake one. New methods also are being developed to gather fingerprint information below the skin surface, charting even pores.

-- Improving image quality. As a way of better using current data, researchers are working on ways to sharpen existing scans and improve the millions of prints in the legacy databases.

-- Combining biometric traits to improve accuracy. Some applications may demand fingerprints and iris scans and facial identification – for added security, or simply for convenience. For example, in a cold climate, it may be preferable to offer an iris scan at times when users don't want to have to remove gloves. Jain says it will be increasingly important to customize methods to meet different needs.

-- Better testing. It will become more important to understand performance on a large scale and what that will mean for actual deployments. Jain pointed out that even a 1 percent failure rate of false positives and false negatives could be disastrous if used at a major airport with high volume traffic.

As commercial uses become more popular, Jain said science will have a greater role not only in improving biometrics, but also accurately representing the strengths and weaknesses of systems.

"Until recently vendors were providing the performance data, but numbers were not realistic," Jain said. "In the field of biometrics the academic community has started playing a role only recently. Vendors don't always have the best interest of science, but are more interested in selling the system and making a profit. Scientists have to tell the honest story and provide realistic performance -- and that it is not foolproof. That it is not foolproof no matter what people say."

Source: Michigan State University

Citation: Biometric science seeks to avert identity crisis (2006, February 20) retrieved 27 April 2024 from https://phys.org/news/2006-02-biometric-science-avert-identity-crisis.html