# One Face in 6 Billion

That's the challenge confronting face-recognition experts who hope to protect us from terrorists—to identify every single human on the planet

SHORTLY AFTER THE TERRORIST ATTACKS ON SEPTEMBER 11, THE FEDERAL BUREAU OF Investigation was reduced to asking Americans if they could identify any of the 19 suspected hijackers. In the months that followed, it became clear that human efforts to track terrorists might not be enough. So it wasn't surprising to see a new technology race develop between at least 20 firms trying to build electronic watchdogs, including face-recognition systems. Before long, some companies proposed that if their systems were installed in airports, just as metal detectors are, hijackers and terrorists could be identified before they boarded planes. Several such systems have been installed on a trial basis.

**Below: Identix (formerly Visionics) software searches a photographic database for a face match. Small images on the left side of the monitors show the last 28 scans; the enlarged face is the current scan. Once a search is complete, the closest matches are displayed in the right-hand field.**

PHOTOGRAPH BY KAI WIECHMANN

But so far none of the face-recognition systems tested in airports has spotted a single person actually wanted by authorities. Instead, they have served only to embarrass innocent people. The technology seems to be better at making incorrect matches, called false positives, than spotting terrorists. Barry Steinhardt, director of the American Civil Liberties Union's Technology and Liberty Program, says tests of face-recognition technology show it is far from effective, and most likely little will be gained in return for surrendering privacy rights and mobility. "Under real-world conditions," he says, "Osama bin Laden could easily evade a face-recognition system."

Although Internet search engines can scan more than a billion documents in a second, and government fingerprint systems can identify a murderer from decades-old fingerprints, matching a person's face against a database of photographs has proved to be remarkably difficult. That flies in the face of common sense because most humans can identify hundreds of different individuals by their faces.

"There is a difference between recognizing people you are familiar with and recognizing strangers," says Charles Wilson, who manages the Image Group at the National Institute of Standards and Technology. Most of the faces people recognize readily are those they have seen in different situations, wearing different clothes, sporting different hairstyles, over many years. Those memories work together. Asking a computer to recognize a hijacker in an airport based on one or two grainy photographs gleaned from a driver's license or a passport, Wilson says, is like trying "to recognize somebody you have glimpsed for only two seconds."

Some of the technology in use today to recognize faces, such as that offered by Viisage Inc., was derived from work done at the Massachusetts Institute of Technology's Media Lab in the late 1980s. Funded by the Nielsen ratings group, the Media Lab was asked to build a television that knew who was watching it. Current Viisage software takes a digital →

→ image of a person's head and searches for the face, then the eyes. It rotates the image so the eyes are horizontal (eliminating the problem of tilted heads) and scales the image so the eyes are a fixed number of pixels apart. This process, called normalizing, is also used on all the images in the database, ensuring that the faces stored will be uniform.

To build the software, designers analyzed photos of hundreds of thousands of faces and boiled them down to 128 different basic images, called eigenfaces. Taken together, they are meant to represent the full range of facial physiognomy. The normalized image is compared with all the eigenfaces and coded to create a template, which can then be used in one of two ways. When the system needs to verify that a person is who he or she claims to be—for example, that an airport maintenance worker beginning a shift is, in fact, that worker—this template is compared with a stored template of that person's face. If enough measurements are similar, the two are declared a match. When the system needs to identify a person—to check, for instance, whether a passenger boarding a plane is among those on a watch list of terrorists and other criminals—the template of the passenger in question is compared with all templates in the database. The computer displays templates that correspond most closely to the passenger's template. Then a security officer must decide if there seems to be a match.

'IF YOU LOOK LIKE A TERRORIST ON DAY ONE, YOU'LL LOOK LIKE A TERRORIST 10 DAYS FROM NOW'

Viisage competes primarily with Identix, a company that uses a system based on research developed in part by physicist Joseph Atick, the company's chief executive officer. The Identix approach is in some ways similar to Viisage's. First, a digital image is acquired, then normalized, reduced to a code, and compared with others in a database. But the Identix system generates that code differently. Instead of relying on eigenfaces, Identix uses a technique called local feature analysis, measuring up to 80 distances between facial features, such as from the cheekbone to the bridge of the nose. The measurements are coded and then compared with values assigned to images in the database to determine whether a match exists.

Both systems work well under ideal conditions, but putting face recognition into play in the real world is problematic. Creating a useful database is daunting if not impossible. Photographs of known terrorists can be fed into the system, but only a small fraction of terrorists have ever been identified.

Even if a terrorist's photo does reside in a database, other variables make a successful match unlikely. A match may depend on lighting conditions. Features like a person's nose can cast a shadow if the light hits the face from an angle different from that of the original scan. A beard, glasses, a suntan, or makeup may throw off a match, as can a slight change like turning one's head to the side.

Perhaps the most mundane challenge to face recognition is aging. Faces change dramatically during adolescence and gradually in adulthood. If a face is scanned every day and the image in the database is updated, a face-recognition system may be reasonably accurate. Because terrorists could try to disguise themselves as airport personnel, face recognition might be effective for screening workers as they come on the job.

False negatives—matches that don't happen and should—are disturbing because they mean criminals can slip through the net. False positives, on the other hand, disrupt the lives of ordinary citizens. Steinhardt argues that inaccurate matches present a challenge to freedom. During a test at the Palm Beach Airport in Florida, the Identix system produced a false positive more than twice an hour, and it was able to identify only 47 percent of the time the 15 employees who had volunteered to pose as terrorists on a watch list. In May the airport announced it would not adopt the system.

In another test, Identix software was installed last December by Pelco of Fresno, California, at the Fresno Yosemite International Airport. It generates about one false positive for every 750 passengers scanned, says Pelco vice president Ron Cadle. Shortly after the system was installed, a man who looked as if he might be from the Middle East set the system off. "The gentleman was detained by the FBI, and he ended up spending the night," says Cadle. "We put him up in a hotel, and he caught his flight the next day." Cadle adds that extreme cases are likely to be exceptions. Most matches can be "cleared," he says, by pulling the person to one side, then "running them through again." Atick defends the Identix software, saying it "is not an identification system. It is an alarm system." He says the software can deliver an error rate of only three false positives in 200. That rate, he says, need not disrupt the flow of passengers onto aircraft. But if a passenger gets a false-positive match once, says Samir Nanavati, founding partner of the International Biometric Group, a consulting firm in New York, that person should get one every time he flies. "If you look like a terrorist on day one, you are going to look like a terrorist 10 days from now."

Although face-recognition technology is likely to continue improving, there are too many ways to get around even the best designed and most carefully installed system. What may be more important in the short term is to acknowledge that software won't be a quick fix for aviation security. Embracing it immediately might provide little more than what Nanavati deems "a dangerous illusion of security." ☒

**Every new U.S. passport must contain a biometric—a facial scan, fingerprint, or retinal scan—after October 26, 2004. The key, says Charles Wilson of the National Institute of Standards and Technology, is speed: "An INS inspection has to take less than 13 seconds, or the border backs up."**