May 31, 2004

Technology Strains to Find Menace in the Crowd

By BARNABY J. FEDER

Face-recognition technology, often touted as a promising tool in the fight against terrorism, earned a bad reputation after it failed miserably in some well-publicized tests for picking faces out of crowds. Yet, on simpler challenges, the technology's performance is improving and business has been growing.

Major casinos now use the technology to spot card counters at blackjack tables. Washington is planning to require the technology in the next generation of American passports. Several states are using face-recognition systems to check for individuals who have obtained multiple driver's licenses by lying about their identity. And Pinellas County, Fla., recently began deploying the system in police cars so officers can check the people they stop against a database of photographs without having to go back to the office.

Face-recognition systems, using cameras and computers to map someone's facial features, collect the data for storage in databases or on a microchip on documents like passports. Making the technology work has required nearly perfect lighting and cooperative subjects, conditions that are not present when trying to spot suspected terrorists and criminals in a crowd.

That kind of application, however, remains a goal. This summer, the National Institute of Standards and Technology will stage a competition, challenging vendors to cut error rates on systems it tested in 2002 by at least 90 percent, with the results to be published next year. The prize for top performers - bragging rights based on impartial tests - is a valuable marketing tool in an industry filled with small companies.

For now, sellers of the technology have to deal with much skepticism. "The companies have not done a good job of positioning it, and as a result the technology has gotten a black eye," said Thomas J. Colatosti, a security consultant who was formerly the chief executive of Viisage, one of the few publicly traded companies in the business.

The most damaging publicity came from tests of face-recognition software and video-surveillance cameras used to spot criminal suspects on the streets of Tampa, Fla., and Virginia Beach. Those programs have not led to a single arrest, but have angered privacy advocates. Another face-recognition system that scanned 100,000 football fans entering the 2001 Super Bowl in Tampa picked out 19 people with criminal records, but none were among those being sought by the authorities.

Nonetheless, major integrators of security technology for governments, like the Unisys Corporation, Honeywell International and I.B.M., all support face-recognition technology for some uses. Viisage, based in Billerica, Mass., has seen its stock price double this year, and shares of its major domestic rival, Identix, based in Minnetonka, Minn., have also risen sharply. Viisage closed Friday at $9.81 a share, down 26 cents, or 2.6 percent, on the Nasdaq.

Though the sector remains volatile, some of the strength of those two stocks reflects the success of the

companies in diversifying away from dependence on face recognition, said Joel P. Fishbein Jr., who follows security technology for Janney Montgomery Scott, a brokerage firm in Philadelphia that makes a market in the stocks but does not own any of them. Mr. Fishbein added that there is a high percentage of short sellers in the market, who are betting the prices will tumble.

Skepticism has also made it hard for entrepreneurs attempting to break into the field with new innovations.

"It soured the whole market," said Lawrence Schrank, co-founder and chairman of 3DBiometrics, a recent start-up in Boulder, Colo., that is pursuing the use of lasers to map facial structures. Dr. Schrank, a former researcher at Xerox Parc, said that the technology, currently used in medical-imaging equipment, could help the military identify individuals at long distances.

Since the Sept. 11, 2001, terrorist attacks, there have been numerous trials of identity-verification technologies at airports. Some trials involved matching volunteers posing as terrorist suspects to file photos of them on a watch list. Others tried to match authorized personnel like flight crews with photo databases.

The biggest problems were the large number of "suspects" and unauthorized people who passed through control points undetected. Critics, like the American Civil Liberties Union, have also complained that the systems routinely generate a smaller number of "false positives," which mistakenly identify innocent people as suspects.

Analysts and many industry officials say that too much is being expected from the technology, which is still one of the newest methods in biometrics, a field that includes analysis of fingerprints, voices, hand shapes, gait and patterns of the iris.

The total biometrics market this year will reach about $1.2 billion, with face-recognition systems accounting for $144 million, according to projections by the International Biometric Group, a research company in New York. Face-recognition revenues should double next year and climb to more than $800 million by 2008, according to International Biometric.

Advocates of face-recognition technology have long promoted it as one of the least intrusive biometrics, and potentially the most powerful because it can make use of a huge amount of existing data.

"There are 1.2 billion digitized photos of people in databases around the world," the chief executive of Identix, Joseph J. Atick, said.

In the late 1990's, entrepreneurs in the field raced to come up with the best mathematical formula for accurately describing a face and the software for quickly measuring it against databases. Pioneers like Dr. Atick played down the difficulty of getting useful images, contending the systems measured so many variables that they would be hard to deceive.

Experience showed otherwise. Performance plummeted in poor lighting, when subjects moved past control points without staring directly into the cameras and when eyeglasses or other objects covered part of the face. Success rates also declined as the databases of potential matches grew and as the photos used got older.

Government-sponsored testing revealed other unexplained anomalies, like the tendency of the systems to identify men more accurately than women, and Asians more accurately than other races.

Technology sellers are pursing a variety of strategies to improve the results. Some are developing systems that start with three-dimensional images taken by multiple cameras, allowing more varied head angles as a person

walks through a checkpoint. Others are developing complex mathematical functions to transform two-dimensional images into three-dimensional models. They are also using software to compensate for poor lighting and to take shadows off a face.

The technical advances are having an impact. Viisage, for example, struggled to achieve a 50 percent recognition rate in tests last year at Boston's Logan International Airport. But Mohamed Lazzouni, the company's chief technology officer, claimed that Viisage's results would improve to better than 90 percent if it repeated the trial with its latest technology, including elements brought in when it acquired ZN Vision Technologies of Germany in January.

Combining face recognition with other biometrics or even nonbiometric security measures could also improve the success rate. Identix hopes to meet the goal set by the National Institute of Standards and Technology by combining a technology for measuring skin texture with its FaceIt feature mapping system, Dr. Atick said.

Last year, the International Civil Aviation Organization, a division of the United Nations, adopted the use of dual biometrics in passport standards. That agency's decision to have face-recognition technology and fingerprints incorporated in all passports has been endorsed by the United States, which recently began laying the groundwork for adding face recognition to fingerprinting in all visa applications.

Those documents will eventually contain microchips recording lasting facial characteristics like the distance between eyes and shape of the jaw. Scanners at check-in counters could then check whether the face of the traveler bearing the document matches the data on the chip.

But the challenge of including the technology in passports is still enormous. The Bush administration told Congress that neither the United States nor any other country could comply with the Oct. 26 deadline Congress had set for all travelers who do not require a visa to enter the United States to have the new biometrically equipped passports.

Most experts say including face data on microchips in passports will take at least another year, and deploying the systems needed to analyze the data at every port of entry could be delayed for years.