 By Warren Webb, Technical Editor

Friend or Face recognition goes to war

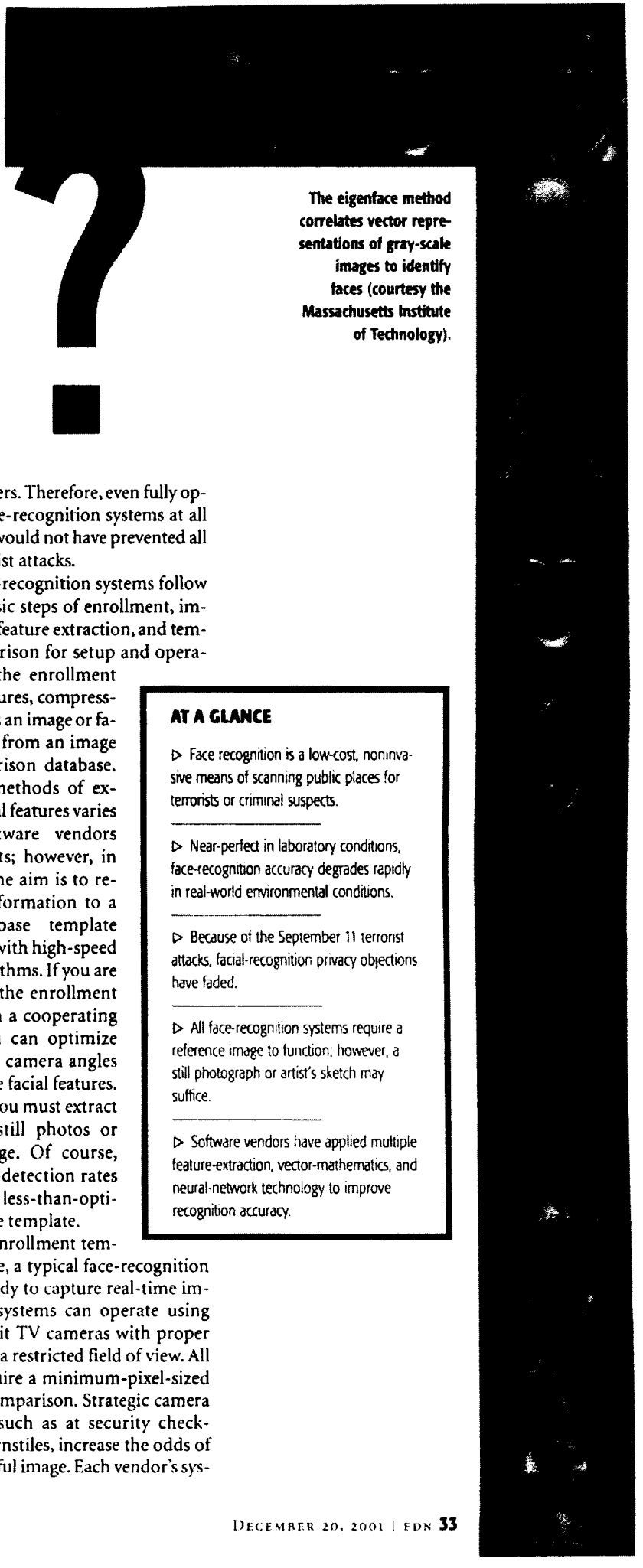
HOBBLED BY PRIVACY ISSUES BEFORE THE SEPTEMBER 11 ATTACKS, FACE-RECOGNITION TECHNOLOGY HAS SUDDENLY JUMPED TO THE FOREFRONT OF THE WAR ON TERRORISM.

THERE HAS BEEN A MAJOR CHANGE in attitudes about security technology since the terrorist attacks on the World Trade Center and the Pentagon. Invasive technologies that were once in the "Big Brother" category are now a small price to pay for the American way of life. Face recognition is one of these technologies with the potential to take away a criminal's favorite cover: hiding within a crowd of people. Armed with a database of photos, face-recognition systems can constantly scan public areas to identify and notify authorities of wanted criminals or terrorists. In addition to crime fighting, face-recognition technology can also find use in more mundane security applications, such as identification, access control, and authentication.

Before the attacks, face recognition was a controversial and obscure technology used mainly in casinos to identify cheaters and high rollers. In fact, privacy advocates soundly criticized pilot programs at the 2001 Super Bowl and on the streets of Tampa, FL, even though these systems identified a few wanted suspects. Borders bookstores suspended a trial plan to implement face-recognition software for loss prevention pending review of legal and human-rights issues. However, after the devastation of September 11, airline passengers and government officials are now ready to trade some civil liberties for tighter security.

Face recognition is one of many biometric-identification techniques, along with fingerprint recognition, handwriting analysis, iris or retina scans, voiceprints, and DNA analysis. All of these forms rely on human biological characteristics and require previous knowledge of the subject. Face recognition is unique in that a simple still photograph provides enough information for real-time comparison with live candidates. Also, face-recognition systems do not require cooperative subjects, because strategically placed cameras can covertly scan every passerby. In many cases, especially with suspected terrorists, authorities do not have fingerprints or other biometric information, but they do have pictures.

foe?



The eigenface method correlates vector representations of gray-scale images to identify faces (courtesy the Massachusetts Institute of Technology).

Therefore, face recognition becomes an important identification tool. Some face-recognition systems function even with an artist's composite sketch.

In addition to its nonintrusive and potentially covert features, face-recognition technology has several other advantages for prospective adopters. Most systems use low-cost, easily installed cameras or closed-circuit TV infrastructures to minimize deployment outlay. Unlike other biometric-identification methods, such as DNA analysis, face recognition and detection are nearly instantaneous, so results can be displayed while the subject is still in the vicinity of the camera. Test or trial systems are also easy to implement, requiring little more than a PC, a PC camera, and demonstration software from a face-recognition vendor.

LIGHTS, CAMERA, ACTION

Although face-recognition software developers can demonstrate near-perfect results in controlled environments, detection rates fall off rapidly in real-world conditions. Inconsistent lighting is one of the biggest problems with recognition systems, because variable shadows can mask facial characteristics. Variations in head orientation also produce degraded results as the captured image deviates from the reference image. Orientation is especially important when you're trying to capture images without a subject's cooperation. Disguises, hats, sunglasses, and face-obscuring hairstyles affect all systems to some extent, although some vendors claim less sensitivity. And, of course, face-recognition systems are worthless without reference images. Before the terrorist attacks, the CIA's watch database contained photos of only two of the 19 hijackers. Therefore, even fully operational face-recognition systems at all US airports would not have prevented all of the terrorist attacks.

Most face-recognition systems follow the same basic steps of enrollment, image capture, feature extraction, and template comparison for setup and operation. First, the enrollment process captures, compresses, and stores an image or facial features from an image in a comparison database. The exact methods of extracting facial features varies among software vendors and products; however, in every case the aim is to reduce the information to a small database template compatible with high-speed search algorithms. If you are conducting the enrollment process with a cooperating subject, you can optimize lighting and camera angles to emphasize facial features. Otherwise, you must extract data from still photos or video footage. Of course, recognition-detection rates suffer with a less-than-optimal database template.

With an enrollment template in place, a typical face-recognition system is ready to capture real-time images. Most systems can operate using closed-circuit TV cameras with proper lighting and a restricted field of view. All systems require a minimum-pixel-sized image for comparison. Strategic camera placement, such as at security checkpoints or turnstiles, increase the odds of getting a useful image. Each vendor's sys-

AT A GLANCE

- ▷ Face recognition is a low-cost, noninvasive means of scanning public places for terrorists or criminal suspects.
- ▷ Near-perfect in laboratory conditions, face-recognition accuracy degrades rapidly in real-world environmental conditions.
- ▷ Because of the September 11 terrorist attacks, facial-recognition privacy objections have faded.
- ▷ All face-recognition systems require a reference image to function; however, a still photograph or artist's sketch may suffice.
- ▷ Software vendors have applied multiple feature-extraction, vector-mathematics, and neural-network technology to improve recognition accuracy.

tem has different requirements for minimum number of pixels, color or gray-scale image, and head orientation for successful detection. It is a difficult task to identify a face against the background clutter in a typical video image, and each vendor offers proprietary algorithms to identify the eyes and then isolate the facial features.

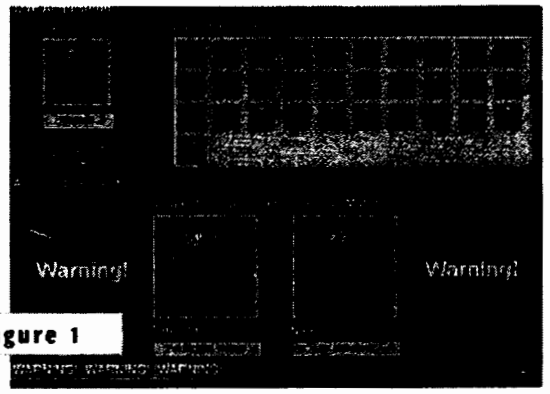


Figure 1

Security personnel secretly scanned thousands of faces at the 2001 NFL Super Bowl using the FaceFinder software system from Viisage Technology.

The real-time feature-extraction process duplicates the enrollment algorithms to generate a small, template-sized representation of the captured facial image as the subject passes the camera. Face-recognition researchers and software vendors have devised several competing techniques, each with advantages and limitations, for extracting facial features and compressing the results. The primary techniques for face recognition include local-feature analysis, *eigenface* (German for one's "own face"), and neural networks. Current off-the-shelf recognition products are based on one or a combination of these techniques. All systems concentrate on portions of the face that are unlikely to change, such as the eyes, cheekbones, and edges of the mouth and de-emphasize hairstyles, facial hair, and eyewear. The key to each technology is to retain enough information to ensure that the system discerns between potentially thousands of faces while minimizing the template size.

MATCHING TEMPLATES

The final step in face recognition is to scan the database and compare the captured-image template. If you're using the system for identity verification, it simply compares the image with a single template to produce a "yes" or "no" response. However, if the primary purpose of the system is to determine a subject's identification, it must compare the image with each template in the database. The system uses multiple frames of a video image to check for minor face movements to differentiate between a photo and a live subject. Search speed, which depends on the size of the database, promises to become a critical factor as localities adopt face-recognition technology and combine data. Most vendors incorporate an adjustable threshold in database searches to display the most likely matches and leave the final selection to a human operator.

Local-feature analysis, the most intuitive of the recognition schemes, records the relative locations of as many as 80 prominent facial landmarks, such as eyes, eyebrows, mouth, tip of the nose, bridge of the nose, and cheekbones. In operation, the system compares facial features from a test subject, along with slight variations to account for changes in expression, with a database of these relative distances. Dark glasses, makeup, or facial hair do not preclude detection, because local-feature-analysis vendors claim that their products can identify a face with a few as 12 to 20 of the 80 landmarks. Local-feature-analysis systems can also accommodate head orientations that vary on either side of a direct frontal image.

FaceIt, a local-feature-analysis-recognition system from Visionics, maps an individual's features into a 3.5-kbyte full template and a smaller 84-byte vector template. The smaller template globally searches an entire database for candidate matches, and the larger template then isolates the best match. Visionics claims that its system is resistant to changes in lighting, skin tone, eyeglasses, facial expression, and hair, and it tolerates pose variations of 35° in all directions. Several law-enforcement agencies, including the New Jersey State Police; the Arizona Department of Public Safety; and sheriff departments in Los Angeles, San Antonio, and Kent County, MI, are using FaceIt. One of the first airport installations for face recognition at Keflavik, Iceland, also used the product. Visionics also offers FaceIt NT Eval to replace desktop-login passwords with automatic face finding and face recognition. The system stores images of people who have attempted access for later viewing.

The eigenface-recognition method, developed at the Massachusetts Institute of Technology, uses a gray-scale image of the entire face instead of individual facial

WHAT'S NEXT? THE ULTIMATE BIOMETRIC

Although face-recognition technology can covertly identify suspects, it gives no information about the other 99.9% of subjects passing before a camera. This situation may soon change. Researchers at Pennsylvania State University (University Park, PA) are working on a system that can—by secretly testing trace elements in the air around your body—determine whether you have been in contact with explosives and chemical or biological agents (Reference A).

Mechanical-engineering professor Gary Settles has been studying the natural plume of warm air that rises from the head and shoulders of every human. This warm air, which rises as high as six feet, contains microscopic flakes of skin and traces of materials the subject has contacted. Settles is working with the FAA to develop an airport portal that will capture and analyze these particles from passengers before they board an aircraft.

This type of particle-analysis system has the advantage of eliminating security profiling, but privacy advocates may still protest its use. In addition to testing for the particles that provide clues to terrorist threats, Settles' portal can also test for drugs, diseases, skin disorders, some cancers, and diabetes and can even capture samples of your DNA. Some insurance companies may find this type of data very interesting. How much personal information are you willing to surrender to board an airplane?

REFERENCE

A. Pennsylvania State University State Online Research, www.rps.psu.edu/0109/portal.html.

features. The basic concept is to represent each image as a vector, so that the system can mathematically compare faces. Because all faces have a similar structure (eyes, noses, mouths, and others), the system correlates the vectors representing them. The search algorithm looks for maximum correlation to confirm a match. Although variations in lighting and head orientation reduce the accuracy of the eigenface approach, you can minimize the inaccuracies by capturing multiple poses of the subject during enrollment.

The ID-2000 system from Imagis Technologies combines face-recognition software with database retrieval of detailed personnel records.

SUPER BOWL SCAN

Viisage Technology has adapted MIT's eigenface method to develop a series of commercial face-recognition products, including the FaceFinder system that authorities used at the 2001 NFL Super Bowl to scan thousands of faces (**Figure 1**). Although the system identified 19 people with outstanding warrants, authorities made no arrests. Viisage and Visionics will compete in a test run to evaluate face-recognition performance at Boston's Logan International Airport. Viisage also has products for physical-access control, point-of-sale identification, and image-database research.

Software vendors have also combined neural-network techniques with local-feature analysis or eigenface methods to improve detection rates. Neural networks require a training session to adjust internal comparison weights for optimal performance. The idea is that performance will improve over time as success and failure data is fed back to the system. The TrueFace recognition engine from eTrue includes a series of neural-network components to customize identity-verification applications (**Figure 2**). The TrueFace engine is a C-callable, 32-bit DLL for Microsoft Windows or a static library for Sun Solaris. The engine supports 36 popular image formats and compression schemes and includes a demonstration program, sample face images, example application-interface source code, and documentation.

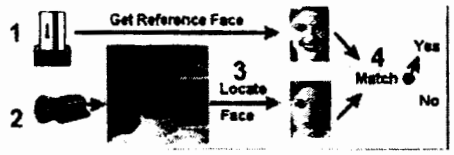


Figure 2 **The TrueFace recognition engine from eTrue allows developers to integrate neural-network components into custom identity-verification applications.**

Since 1993, the US Department of Defense has been involved in the development and evaluation of facial-recognition systems to assist security, intelligence, and law-enforcement personnel in the performance of their duties (**Reference 1**). Last year, the Defense Department sponsored the Facial Recognition Vendor Test to provide the counterdrug community and government agencies with information to assist their efforts in determining where facial-recognition technology would best be used in the field. The test was administered in May and June 2000 and assessed the capabilities of facial-recognition systems that were currently available for purchase on the US market. Although the tests were not designed to provide a buyers' guide to the best products, they did provide a standard method of evaluating systems.

Face recognition is difficult even for humans, because many of us look alike. Everyone has heard that they look like a relative or a celebrity. Similarly, we have all had trouble identifying faces from an old class photo. Hundreds of people have enough similar features to fool or confuse today's face-recognition technology. In fact, reliability is the biggest problem with face-recognition systems, and variables such as lighting, pose, expression, temporal variation, camera distance, and subject participation compound the problem.

Even with perfect detection, a face-recognition system won't prevent crimes or terrorism, because it does not detect a subject's intent. Face recognition will never be a complete answer to crime or terrorism prevention (see **sidebar** "What's next? the ultimate biometric"). However, it may become an effective tool as techniques improve and when vendors combine it with other biometric-screening techniques. As with any new technology, it will take time for the public to adjust to and accept the changes. Airports had little security 20 years ago, yet everyone today expects their carry-on items to be X-rayed and possibly searched. Likewise, face recognition will become part of our future national-security systems.□

You can reach Technical Editor Warren Webb at 1-858-515-3713, fax 1-858-486-3646, e-mail wwwebb@cmp.com.

FOR MORE INFORMATION...

For more information on products such as those discussed in this article, go to www.ednmag.com and click on the Reader Service link under the Tools & Services section. When you contact any of the following manufacturers directly, please let them know you read about their products in *EDN*.

eTrue Inc
1-508-303-9901
www.etrue.com
Enter No. 301

Viisage Technology Inc
1-978-952-2200
www.viisage.com
Enter No. 303

Imagis Technologies Inc
1-604-684-2449
www.imagis-cascade.com
Enter No. 302

Visionics Corp
1-201-332-9213
www.visionics.com
Enter No. 304

SUPER INFO NUMBER
For more information on the products available from all of the vendors listed in this box, go to www.ednmag.com, click on the Reader Service link, and enter no. 305

REFERENCE

1. Department of Defense Counterdrug Technology Development Program Office, www.dodcounterdrug.com/facialrecognition/.