findBIOMETRICS.com
complete identification verification resource

. biometrics .

Facial Recognition - Guides and Articles

Q&A on Facial Recognition

What is facial recognition technology?
Facial recognition systems are built on computer programs that analyze images of human faces for the purpose of identifying them. The programs take a facial image, measure characteristics such as the distance between the eyes, the length of the nose, and the angle of the jaw, and create a unique file called a "template." Using templates, the software then compares that image with another image and produces a score that measures how similar the images are to each other. Typical sources of images for use in facial recognition include video camera signals and pre-existing photos such as those in driver's license databases.

How is facial recognition technology currently being used?
Unlike other biometric systems, facial recognition can be used for general surveillance, usually in combination with public video cameras. There have been three such uses of face-recognition in the U.S. so far. The first is in airports, where they have been proposed - and in a few cases adopted - in the wake of the terrorist attacks of September 11. Airports that have announced adoption of the technology include Logan Airport in Boston, T.F. Green Airport in Providence, R.I., and San Francisco International Airport and the Fresno Airport in California.

A second use of the technology was at the 2001 Super Bowl in Tampa, where pictures were taken of every attendee as they entered the stadium through the turnstiles and compared against a database of some undisclosed kind. The authorities would not say who was in that database, but the software did flag 19 individuals. The police indicated that some of those were false alarms, and no one flagged by the system was anything more than a petty criminal such as a ticket scalper. Press reports indicate that NewOrleans authorities are considering using it again at the 2002 Super Bowl.

The technology has also been deployed by a part of Tampa, Ybor City, which has trained cameras on busy public sidewalks in the hopes of spotting criminals. As with the Super Bowl, it is unclear what criteria were used for including photos in the database. The operators have not yet caught any criminals. In addition, in England, where public, police-operated video cameras are widespread, the town of Newham has also experimented with the technology.

How well does facial recognition work?
Computers can do increasingly amazing things, but they are not magic. If human beings often can't identify the subject of a photograph, why should computers be able to do it any more

Showcases
Fingerprint
Iris Recognition
Hand & Finger
Facial Recognition
Voice/Speaker
Consultants
Smart Cards/Multimodal
Signature/Keystroke
2D Bar Codes

reliably? The human brain is highly adapted for recognizing faces - infants, for example, remember faces better than other patterns, and prefer to look at them over other patterns. The human brain is also far better than computers at compensating for changes in lighting and angle. The fact is that faces are highly complex patterns that often differ in only subtle ways, and that it can be impossible for man or machine to match images when there are differences in lighting, camera, or camera angle, let alone changes in the appearance of the face itself.

Not surprisingly, government studies of face-recognition software have found high rates of both "false positives" (wrongly matching innocent people with photos in the database) and "false negatives" (not catching people even when their photo is in the database). One problem is that unlike our fingerprints or irises, our faces do not stay the same over time. These systems are easily tripped up by changes in hairstyle, facial hair, or body weight, by simple disguises, and by the effects of aging.

A study by the government's National Institute of Standards and Technology (NIST), for example, found false-negative rates for face-recognition verification of 43 percent using photos of subjects taken just 18 months earlier, for example. And those photos were taken in perfect conditions, significant because facial recognition software is terrible at handling changes in lighting or camera angle or images with busy backgrounds. The NIST study also found that a change of 45 degrees in the camera angle rendered the software useless. The technology works best under tightly controlled conditions, when the subject is starting directly into the camera under bright lights - although another study by the Department of Defense found high error rates even in those ideal conditions. Grainy, dated video surveillance photographs of the type likely to be on file for suspected terrorists would be of very little use.

In addition, questions have been raised about how well the software works on dark-skinned people, whose features may not appear clearly on lenses optimized for light-skinned people.

Samir Nanavati of the International Biometric Group, a consulting firm, sums it up: "You could expect a surveillance system using biometrics to capture a very, very small percentage of known criminals in a given database."

What is the government's previous experience with facial recognition?

Several government agencies have abandoned facial-recognition systems after finding they did not work as advertised, including the Immigration and Naturalization Service, which experimented with using the technology to identify people in cars at the Mexico-U.S. border.

However, the government also has possession of a huge, ready-made facial image database - driver's license photos - and is looking into how they can be used. By law, the government can't sell those photos to private companies, but there are no prohibitions on their use for surveillance purposes by the government itself. The Federal government has begun to fund pilot projects on expanding the use of driver's license photos to facial recognition databases.

Should we deploy face-recognition in airports to prevent terrorism?
It makes no sense to use face-recognition in airports. To begin with, there is no photo database of terrorists. Only two of the 19 hijackers on September 11 were known to the CIA and FBI - and surviving terrorists aren't exactly lining up to have their photo taken by the U.S. government. In addition, the technology simply isn't reliable enough for such an important security application. It would work especially poorly in the frenetic environment of an airport, where fast-moving crowds and busy background images would further reduce its already limited effectiveness. The evidence suggests that these systems would miss a high proportion of suspects included in the photo database, and flag huge numbers of innocent people - lessening vigilance, wasting precious manpower resources, and creating a false sense of security.

Should we use the technology in other public places?
If facial recognition is unjustified in airports and at public events such as the Super Bowl, its use for general surveillance is even more inappropriate. The security threat on a public street is far lower than in airports, and sociological studies of closed-circuit television monitoring of public places in Britain have shown that it has not reduced crime. The balance between the risks and benefits of facial recognition is even more unfavorable in such locations than in airports.

How does facial recognition technology threaten privacy?
One threat is the fact that facial recognition, in combination with wider use of video surveillance, would be likely to grow increasingly invasive over time. Once installed, this kind of a surveillance system rarely remains confined to its original purpose. New ways of using it suggest themselves, the authorities or operators find them to be an irresistible expansion of their power, and citizens' privacy suffers another blow. Ultimately, the threat is that widespread surveillance will change the character, feel, and quality of American life.

Another problem is the threat of abuse. The use of facial recognition in public places like airports depends on widespread video monitoring, an intrusive form of surveillance that can record in graphic detail personal and private behavior. And experience tells us that video monitoring will be misused. Video camera systems are operated by humans, after all, who bring to the job all their existing prejudices and biases. In Great Britain, for example, which has experimented with the widespread installation of closed circuit video cameras in public places, camera operators have been found to focus disproportionately on people of color, and the mostly male operators frequently focus voyeuristically on women.

While video surveillance by the police isn't as widespread in the U.S., an investigation by the Detroit Free Press (and followup) shows the kind of abuses that can happen. Looking at how a database available to Michigan law enforcement was used, the newspaper found that officers had used it to help their friends or themselves stalk women, threaten motorists, track estranged spouses - even to intimidate political opponents. The unavoidable truth is that the more people who have access to a database, the more likely that there will be abuse.

Facial recognition is especially subject to abuse because it can be used in a passive way that doesn't require the knowledge, consent, or participation of the subject. It's possible to put a camera up anywhere and train it on people; modern cameras can easily view faces from over 100 yards away. People act differently when they are being watched, and have the right to know if their movements and identities are being captured.

The bottom line: how do we decide whether to install facial recognition systems?
Facial recognition - or any security technology - should not be deployed until two questions are answered. First, is the technology effective? Does it significantly increase our safety and security? If the answer is no, then further discussion is beside the point. If the answer is yes, then it must be asked whether the technology violates the appropriate balance between security and liberty. In fact, facial recognition fails on both counts: because it doesn't work reliably, it won't significantly protect our security - but it would pose a significant threat to our privacy.

Source: American Civil Liberties Union

back
