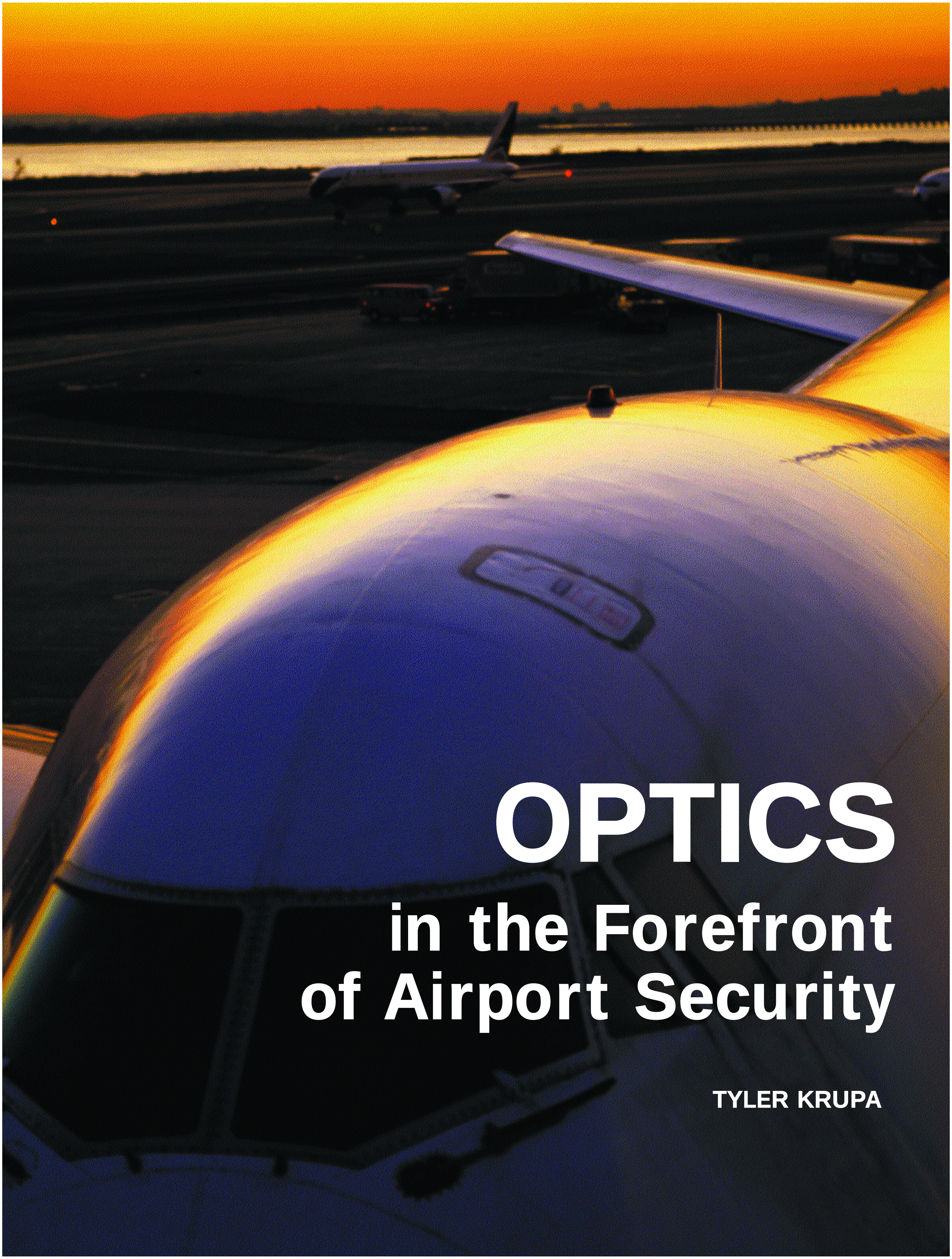


OPTICS

in the Forefront of Airport Security

TYLER KRUPA

In the near future, biometric identification systems based on optical technologies could well play a major role in safeguarding airports from terrorist attacks. Biometric identification systems,including electronic fingerprinting, facial recognition software, and iris scanning equipment, use optics to identify people by their physical characteristics. Such systems have been used for years in high-security areas such as government intelligence posts and military bases. In the wake of the September 11 terrorist attacks that leveled the World Trade Center and damaged the Pentagon, the International Air Transport Association (IATA) has called for the introduction of such systems in airports. Coupled with enhanced detection equipment to alert security personnel to the presence of hidden weapons, biometric technologies could prove to be a viable,long-term solution to the problem of guaranteeing airline safety.

In the future, airport security checks may include electronic fingerprint scans. (*Source:PhotoDisc*)

Electronic fingerprinting

Electronic fingerprinting is one of the biometric airport security systems being proposed by IATA. If the system were to be adopted on a widespread basis, airline personnel (who are already required to be fingerprinted in the context of criminal background checks) would be issued "smart" identification cards containing electronic scans of their fingertips. To gain access to sensitive areas like baggage hangars, a worker would first need to have his or her fingerprints read by a tiny scanner situated either on a locked door or in a small box nearby. If the scan did not match the electronic record in the card, the door to the secure area would remain locked.

Following the September 11 attacks, seven U.S. airports—including Boston's Logan International, JFK in New York,and Chicago's O' Hare—installed or ordered fingerprint scanners to protect security-sensitive areas. At sites where the systems have already been installed, workers place their fingers on small black boxes outside the access points to restricted areas. The scanners take an image of their fingerprints by reading the "minutia points," 30 to 40 breaks and splits unique to every person. The technology "reads" the breaks and converts them into a computer algorithm that is then matched against a database of other fingerprints.

In the wake of the September 11 terrorist attacks that leveled the World Trade Center and damaged the Pentagon, the International Air Transport Association (IATA) has called for the introduction of biometric systems in airports.

In addition to this technology, which is already being used to identify airport and airline employees, frequent airline travelers can bypass immigration procedures at nearly a dozen North American airports by registering their palm prints with the Immigration and Naturalization Service (INS). Thanks to palm screening, passengers known to immigration officials or to the airlines are removed from the pool of those who need to be checked, allowing more resources to be devoted to checking other passengers. Since fingerprints have been used as a security method for over a century, law enforcement agencies already maintain numerous databases that can be used to identify criminals.

According to the INS, since some of the hijackers responsible for the September 11 attacks were already on an immigration "watch list," they might have been apprehended before the tragedy if airport fingerprint check systems had been in place. If electronic fingerprinting is adopted on a large scale, passengers could be required to submit to a scan as they check baggage and again as they enter the boarding gate. The collected fingerprint scans would be checked against a database containing the prints of known terrorists.

Certain "landmarks" on a human face can be mapped quickly to match people with a database of images.The software is not fooled by disguises like wigs and beards. (*Source:CNN.*)

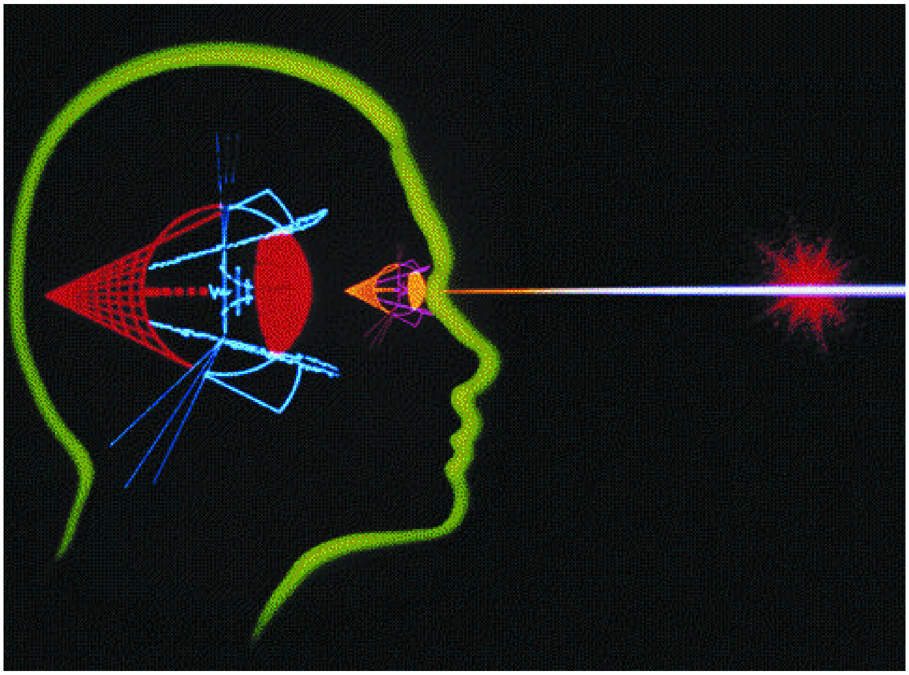
Face recognition

Since authorities in many cases only have pictures of suspected terrorists,face recognition systems, which are also being requested by IATA,may succeed where electronic fingerprinting falls short. Focusing on 80 landmark features—including the bridge and tip of the nose, the size of the mouth and eyes, and the angle of the cheekbones—the computer technology scans faces in crowds and creates face prints that can then be compared to a database of criminals and suspected terrorists.

Face recognition technology, which is not short circuited by the use of wigs or fake beards, converts a photograph or video image of a face into a mathematical algorithm that describes the face's geometric characteristics. The system needs only 14 to 20 landmark features to make a positive match. It has the ability to scan 15 faces simultaneously and compare them to a database of images at the rate of one million faces per second.Once the technology recognizes a face, a silent alarm notifies the authorities.

Face recognition setups at airports would use cameras mounted at gates and terminals to capture images of passengers. A major advantage of such systems is that they are both unobtrusive and passive, allowing authorities to monitor crowds without individuals' direct knowledge or involvement. All images captured by the cameras can be compared with facial template files in the database of known or suspected terrorists and criminals. To date, federal officials have compiled a database of approximately 30,000 wanted individuals.

Keflavik International Airport in Iceland has become the first airport in the world to announce that it has begun using this technology to screen passengers. If the results are positive,I ATA expects that other airports will follow Iceland's lead in the near future. It should be noted however, that while face recognition techniques may be less intrusive, the accuracy level is not as high as with other biometric systems such as fingerprint or iris scanning. Although the error rate for facial matches under optimal conditions can be less than 1%, the accuracy depends on the clarity of both the photos in the database and the images being captured and searched. Low-light conditions or faces recorded at odd angles can lower accuracy rates.



Iris recognition technology examines more than 240 degrees of freedom in the human iris to create a 512-byte data template used to identify individuals or authenticate user privileges. (*Source:PhotoDisc.*)

Eye recognition

Other airport security systems may use eye recognition technology. In these systems a camera reads the unique,distinct patterns of a person's iris, the colored ring around the pupil of the eye. Iris recognition technology examines more than 240 degrees of freedom in the human iris to create a 512-byte data template used to identify individuals or authenticate user privileges. Since no two retinas are alike—not even those of identical twins—retinal scanning is widely recognized as the most accurate of the biometric technologies. Since the vascular pattern in the retina does not change over the course of an individual's lifetime, it constitutes a permanent source for authenticating identity. Another plus: it is virtually impossible to replicate the vascular pattern in the human retina.

Eye recognition technology has already been tested at the airport in Charlotte, North Carolina. As part of a program aimed at speeding the flow of travelers through the airport, prior to flights over 6,000 people submitted "eye prints" to the airlines.Once the passengers arrived at the airport, their eyes were scanned again: in this instance, iris scanning proved to be 100% accurate. Although the iris recognition technology—which cycled through 1,500,000 matches per minute—registered an initial false rejection rate of 1.8%, no users experienced a false rejection after three attempts. The study, sponsored by the Communications Electronics Security Group (CESG), was performed from May to December 2000. It was conducted in accordance with the "Best Practices in Testing and Reporting Performance of Biometric Devices" developed by the British government's Biometrics Working Group.

On the basis of these encouraging results, eye recognition technology is set to go on trial at London Heathrow, Europe's largest airport, in the fall of 2001. As part of a program to speed passengers through customs and immigration control, IATA will test a retinal scanning system on 2,000 passengers who frequently fly into Heathrow on British Airways or Virgin Atlantic. The procedure, developed by EyeTicket Corp. (McLean, Virginia), requires that passengers look into a video camera for two seconds. The system will be fully computerized with voice prompts and auto focus. Each person's distinct iris pattern will be tallied with a passport number and airline check-in computer details. If successful, the technique could be extended to other British and European airports.

Detection systems

In addition to using biometric technologies to identify potential terrorists,airport security can be tightened with enhanced capability to locate hidden weapons. Although metal detectors and x-ray scanners in most airports are quite sophisticated, finding hidden knives is still difficult. Due to the large number of items present in most carry-on baggage, as well as the number of compartments and pockets, weapons such as small knives and box cutters can be difficult to spot. In addition, since many knives are made of non-metallic material,metal detectors are not always of great use.

A number of advanced weapon detection systems may now be introduced to help insure no weapons make it on board an aircraft. One x-ray machine developed by Rapiscan Security Products (Hawthorne, California) is designed for use on passengers rather than carry-on baggage. The machine, which resembles a large gray wardrobe closet, uses a narrow beam of low-powered x rays to scan passengers. The x rays penetrate a few millimeters into the body and reflect back to sensitive detectors. Soft objects such as flesh and clothing reflect weak signals. Dense objects such as guns, knives, or plastic explosives return stronger signals. Advanced software and computers process these signals, producing images in which the hard objects are clearly defined. According to Rapiscan, the three-second exposure to the machine's x rays are not any more harmful than the natural exposure to radiation that most travelers experience in 20 seconds of flight on a conventional airplane.

Researchers at the National Institute of Standards and Technology (NIST, Boulder, Colorado) are also developing a system that will allow security officials to spot concealed weapons. The system uses a form of radar that relies on extremely high-frequency radio waves. The waves penetrate light solids such as clothing but reflect off harder solids like guns or knives. These reflected waves are captured and focused onto a 3-in. silicon wafer that contains 120 antennas tuned to the high frequencies. A set of specially designed electronic boxes interprets these signals into an image, which is subsequently displayed on a laptop computer screen. NIST researchers predict the device will eventually be made small enough for security personnel to hold in their hands.

The device allows researchers to see details by using radio wavelengths first tested by earth-based space observatories to study far-off stars. Astronomers noted that terahertz radio frequencies could penetrate earth's distorting atmosphere but still bring in clear details about distant stars. Since the technology is well researched, NIST scientists predict that adapting it for security applications should not be difficult or costly. The silicon wafers used in the detector, for instance,are created using the same process used to produce computer chips. And unlike typical radar systems that emit hundreds of watts of power, the NIST device puts out much less energy, making it safe for use on people. Although this technology could be some years away from full-scale deployment at airports, NIST researchers estimate that a complete prototype will be ready for testing by the end of 2001.

Other imaging technologies that do not use x rays or radio waves are also becoming available. In collaboration with the National Institute of Justice (NIJ), Trex Enterprises (San Diego, California) is testing a passive millimeter wave camera. Much like an infrared camera, the Trex device can detect hidden objects by measuring differences between the heat energy naturally emitted by a person's body and the concealed object. Any objects that block or attenuate the person's body heat are revealed. Video-rate imagery testing collected in 1999 demonstrated the contraband detection capability of the camera sensor. Since this system emits no harmful waves, the technology may be more agreeable to passengers than systems that use x rays to scan bodies.

X ray of a handbag containing a bomb. (*Source:PhotoDisc*.)

Conclusion

While many security experts believe that biometrics may be the solution to more efficient,safer airports,many civil rights advocates warn that such systems could intrude upon personal liberties. For example,iris recognition and electronic fingerprinting systems for passenger check-in would require an electronic database of each individual passenger's biometrics. If airlines or government agencies were responsible for maintaining that data, a person's travel habits could potentially be tracked and monitored—which some call a violation to the constitutional right to privacy.

Another inhibiting factor may be cost. Today, airline companies are responsible for implementing and staffing the security checkpoints at airports. The cost of installing new biometric security systems may exceed hundreds of thousands of dollars per airport—money that the airlines do not have given the sudden and sharp decrease in air passenger revenue.

IATA members believe the high cost of setting up biometric systems should be weighed against the potential financial loss from future terrorist attacks. The solution, according to Tom Windmuller, program director of IATA's Simplifying Passenger Travel (SPT) initiative, is to use a combination of technologies that can offset the pros and cons of each system. In this scenario, based on cost and efficiency comparisons, airport officials could decide, for example, to use fingerprinting for employee access to secure areas,iris scanning for passenger flow, and face recognition to monitor movement in the airport. Although biometric technology is not perfect and critics say the technology is too invasive, the pressure for greater security measures is at an all-time high. In the light of September 11, some believe Fourth Amendment concerns should be less of a priority. To achieve passenger safety, it may be time to start thinking about boarding planes as a privilege granted only to those who are willing to go through the security system.

Further reading

1. P. Eng,"New technology to boost airport security," on-line URL,http://abcnews.g o.com/sections/scitech/DailyNews/WTC_scannertech010914.html.
2. P.Eng,"Finding a weapon in a crowd," on-line URL, http://abcnews.go.com/sections/scitech/CuttingEdge/cuttingedge010720.html.
3. B.Evangelista,"Tech vs.terrorism," The San Francisco Chronicle, October 2001.
4. D. George, "Airport security aiming for new technologies," on-line URL,http://www.cnn.com/2001/US/10/01/rec.airport.security/.
5. D. George, "Face recognition may enhance airport security," on-line URL,http://www.cnn.com/2001/US/09/28/rec.airport.facial.screening/index.html.
6. D. George, "Eye scans to speed air travel," on-line URL,http://www6.cnn.com/2001/TECH/science/08/01/airports.retina/index.html.
7. A.Grundy, et al.,"Retinal Technologies launches company and revolutionizes biometrics," on-line URL,http://www.retinaltech.com/.
8. L.Jacinto, "Security in new technologies," on-line URL,http://abcnews.g o.com/sections/scitech/CuttingEdge/WTC_biometrics010921.html.
9. R.O'Har row Jr.,"Matching faces with mug shots," The Washington Post,August 2001.
10. A.Whilldin,et al.,"Study shows iris recognition technology is superior among biometrics," on-line URL,http://www.sensar.com/news/releases/051701.html.

Tyler Krupa is the senior science writer at Optics and Photonics News. He can be reached at tkrupa@osa.org.