Photonics Spectra
2009
November
October
September
August
July
June
May
April
March
February
January
2008
2007
2006
2005
2004
2003
2002
2001
2000
1999
1998
1997
1996
BioPhotonics
EuroPhotonics
Photonics Handbook
photonics.com

Related Searches
security ID
smart cards
biometrics
checkpoint

Most Popular Content
Glitter-size Solar Cells
IR Eyes to See Back in Time
Fluorescein Images Graphene
Feds Crack Down on Laser Pointers
Single Nanoparticle Detected

Community Forum
Looking for a second hand Newport controller
How I can simulate with different bitrates
Why is there a loss band in

Photonics Spectra ▸ 2009 ▸ October ▸ Feature Articles
Email | Print | Save | Discuss | Digg | Stumble | Reddit | Subscribe | Advertise

Getting a foot in the door: The role of photonics in modern security systems

Hank Hogan, Contributing Editor, hank@hankhogan.com

In times past, a guard might demand someone entering his domain to "halt and be identified." Today that job is increasingly done by security ID systems using a variety of techniques, including photonic ones such as lasers, optical media and optic sensors. An examination of what is going on shows how photonics plays a role in these systems and what future requirements might be for them.

The demands on ID technologies are growing in many ways. For one thing, there is an increasing need for such systems in traditional settings. For another, identification systems are being employed in more and more areas and for wider and wider uses. As a result, analysts forecast substantial growth.

Charles E. Spear Jr. heads US publishing for IntertechPira in Portland, Maine, a division of Pira International, a market research and technical consulting company in Leatherhead, UK. According to Spear, the group expects the overall market to grow at a compound annual growth rate of just under 12 percent from 2009 through 2014, with smart cards and biometrics growing the fastest.

The company recently published a report putting the worldwide market for personal identification at €4.3 billion ($6.1 billion). This figure includes substrates, bar codes, security inks, digital watermarks, radio frequency ID (RFID), biometrics and smart cards.

Behind this growth are several major trends. One is the increasing world population, which leads to an increased demand for ID documents. Counterbalancing that is the global economic slowdown, which has cut government spending on ID projects as well as consumer spending on travel. Spear added that that interoperability among existing systems, especially for passports and visas, could increase the size of the market.

Security on land and at sea

One reason why the need for security ID systems is increasing is a widening range of increasingly sophisticated applications. Anthony R. Zagami, CEO of Security Identification Systems Corp. (SISCO) in West Palm Beach, Fla., said that his company's credentialing products capture various physical attributes of people, such as their images, fingerprints and retinal patterns. These biometric elements are then incorporated in the ID card or token.

Specialized security ID systems (on counter) are increasingly replacing standard sign-in books and generic temporary badges. Courtesy of SISCO.

Of these, he said, an old standby may be the best. "The photograph is still the well-accepted criterion for identification, both passively by visual observation as well as machine application."

Zemax Dongle Bidirectional
UV-C band LEDs

Photonics Directory
Home
Subscribe
Update your listing

A photograph doesn't require any contact, as can be the case with fingerprints. It also doesn't require that the subject put an eye up against some sort of device, as must be done with a retinal scan. Moreover, with the advent of higher resolution cameras, higher quality photos become possible, which makes both human and machine matching of individuals to their images more precise. As is the case with other imaging tasks, getting the best results requires the right lighting. At times, that may mean the use of near-infrared.

SISCO is a leader in the maritime market, providing the identification used by passengers and crew as they embark and disembark a cruise ship. This task puts a premium on speed because it requires getting thousands of people through a checkpoint in a few hours' time. That means there are only seconds to process each individual.

These checks involve a bar code, which is best read using a laser. To speed things up, the company has developed hardware to read cards no matter how they are inserted into the scanner. This avoids the slowdown that occurs when someone puts the card in the wrong way, only to pull it out and possibly repeat the mistake.

Such products are not intended for high-security, low-traffic areas. Instead, they are designed for the equivalent of getting people into and out of an office building through a lobby. One trend is that such systems are becoming more commonplace, as the traditional sign-in book and temporary badge are replaced.

At right, mobile security ID systems scan cards at remote locations, placing a premium on low-power photonics. Courtesy of SISCO. At left, Costa Rica's DIMEX (foreign resident card) features personalized embedded holograms produced by writing a pattern in optical media on the card. This technology makes the card more resistant to tampering and forgery. Courtesy of LaserCard.

As for the future, mobile systems will be increasingly important. That means that the readers should consume little power and be compact, which has implications for the light sources, sensors and optics. There is promising news for the latter two. "We're starting to get some really good quality shots off these smaller cameras, more so than I ever believed you could get out of a lens that small," Zagami said.

One card to rule them all

Security ID systems also are being put to use to make navigating the cyber-physical world easier. For example, Homeland Security Presidential Directive 12, or HSPD-12, mandates a single secure and reliable ID for federal employees and contractors within an agency. This identifier is to be used for physical and logical access. Thus, a sole token will allow entry to a facility and access to computers, databases and networks. Programs that comply with HSPD-12 are currently being rolled out across the US government.

Thanks to the use of artificial intelligence, video surveillance systems such as AISight from BRS Labs are getting smarter, with the ability to alert with virtually no false alarms. But the technology cannot yet identify subjects at a distance, due in part to imaging capabilities. Courtesy of BRS Labs.

Such a shared ID can eliminate the problem of someone on the outside gaining access using an employee's credentials. "If you're in the building, it won't let anyone use your credentials to connect via the VPN [virtual private network]," said Dilip Sarangan, an industry analyst with Frost & Sullivan, a technology market research firm based in Mountain View, Calif.

Sarangan noted that such a measure would have prevented some of the theft of credit card numbers that has occurred in the past. In those cases, the breach occurred because someone on the outside got into a secure network through a VPN or equivalent using the ID of an employee who was actually at work at the time. Because the system didn't know where the employee was physically, it allowed the logical access.

An advantage of this unified cyber-physical approach is that it gets around some of the problems associated with passwords. Security guidelines say that passwords should be unique to each system or log-in, fairly lengthy, not made up of easily recognizable words or phrases, and changed often. That combination is hard to achieve and to maintain, but a well-designed credential can help.

A better watermark

A key feature of any such ID is that it be resistant to forgery and tampering. Photonics technologies can help on both fronts.

LaserCard Corp., also in Mountain View, has been in the security ID system business for years, electing to encode information in a write once, read many times optical medium. The reason behind this choice is, in part, that the optical method enables greater storage capacity, said the company's chief operating officer, Christopher J. Dyball.

Today, LaserCard's products offer 2.8 MB of storage, far greater than the approximately 72 kB available in smart cards. That extra room makes it possible to store a complete biometric record in an uncompressed format – and not just the extracted features used for matching. That amount of storage space also makes it possible to keep an image of the cardholder on the card. Thus, in one medium, a machine-readable biometric – such as a fingerprint – can be stored, along with a human-viewable photograph or a human-readable signature.

"That image is visible and very difficult to replicate," Dyball said. "It has diffractive characteristics that are very difficult to reproduce by any other method."

The technology used is similar to that employed to burn records onto a recordable compact disc (CD-R) – with some crucial differences. The lasers employed are in the near-infrared, running from 780 to 830 nm, about the same range as in CD-R technology, Dyball said. The biggest difference is that the bit size is 2.5 µm and the track pitch is 12 µm, roughly three to 10 times the equivalent figures for CD-R.

That extra room, along with the use of a large chunk of the possible capacity for error correction, makes the optical stripe much more robust than is the case for the standard office CD-R. That toughness is important, given that LaserCard's products are used as official documents by governments including those of the US, Italy, Saudi Arabia and Angola. These cards must last until they are reissued, a period that can be as long as 10 years.

LaserCard is planning to further improve the security features on its products. The optical medium enables creation of a secondary image, one that will appear only when the illumination is at the correct angle. Although it is possible to view this using nothing more than a laser pointer and a white wall, it would take exceptionally steady hands. So the company is developing a tool to make this easier.

"We will offer a small handheld device with a laser in it, which will allow you to view that secondary diffraction image," Dyball said.

Identification at a distance

Despite their advantages, photonics technologies also have a shortcoming. The cards must be presented to a reader, be it machine or human. The scan can be very fast but it can't happen before then.

But checkpoints can be busy places. An extreme example is the San Ysidro border crossing in the San Diego section of California, used by 17 million cars and 50 million people in 2005. Saving even a bit of transit time can have a large economic impact.

That is one reason why the US has turned to RFID technology, which allows information to be extracted while the ID holder is still in line. Photonics technologies can, of course, make such documents more secure through watermarks and the like.

Photonics technologies have the potential to allow identification at a distance. There are efforts under way to read fingerprints or handprints without contact. It may even be possible to do the same with the face, thereby allowing the use of one of the most unobtrusive methods.

Accomplishing that will not be easy. The face is three-dimensional, but imaging is typically 2-D. Thus, any facial recognition system must transform a 3-D model of the subject's face, captured during enrollment, into a 2-D version that can be compared with what is imaged. The transformation must account for changes in lighting, viewing angle and expression, and for facial alterations such as beards, glasses and movement.

Doing so at a distance requires a high-resolution camera, telescopic optics, plenty of memory and a powerful processor. Things such as gait and body shape also could be used to increase recognition efficiency.

However, even all of that might not be enough. Behavioral Recognition Systems, based in Houston, makes software that learns what is normal in a scene and then reports anything unusual. According to its chief technology officer Eric Eaton, there are distinct challenges to enabling facial recognition at a distance, and today's gold standard systems are not perfect.

"Even people are sometimes tripped up by how similar two different people can look," he said.

The complete article appears in the October 2009 issue of Photonics Spectra. If you do not have a copy of this issue, e-mail us a request. Be sure to include your street address or fax number.

More Feature Articles

A New World of Fiber Sensors | Lasers in solar cell production | A closer look at plastic solar cells | The road to solar cell supremacy