how it works

CAPTURING A FINGERPRINT

IS ONLY HALF THE JOB.

Looking under the surface of fingerprint scanners

By Nicholas Cravotta

TRADITIONAL SECURITY focuses on a secret: You know a password that no one else does. The weaknesses of this system are that you can forget the password or that someone can steal it. To protect passwords, a “token” physically contains the password. For example, you can use a smart card or a Universal Serial Bus (USB) key that holds a password so complex you couldn’t remember it if you tried. However, tokens have a weakness because you cannot verify whether the person using the token has a right to use it.

Enter biometric keys. Every human has several distinct and unique characteristics—from voices to fingerprints. As of yet, for example, fingerprints are extremely difficult to mimic, or “spoof.” Coupled with passwords and tokens, they make robust security a reality.

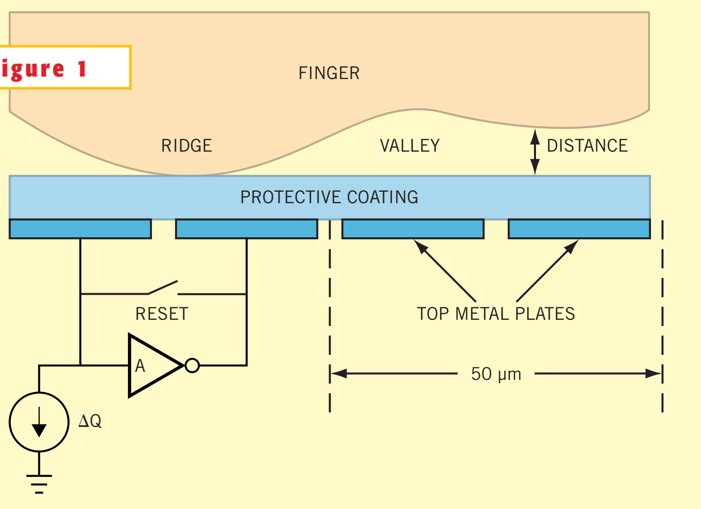
Biometric technology, however, faces difficulties in two key areas: capturing biometric data and accurately recognizing the captured data. Among the current technologies available for using fingerprints as biometric keys, the three main technologies are optical, capacitive, and electric-field (e-field).

OPTICAL SCANNERS

An optical system from Motorola doesn’t use a CCD, as you might expect, but rather uses a monochrome CMOS imager. Instead of supplying data in a bucket-brigade fashion (all pixels read in order), the CMOS imager can address an array of pixels, allowing it to capture an area of interest.

First, the sensor detects when a user places a finger on the plastic for scanning. The finger blocks ambient light, telling the sensor that it is time to scan. Surface-mounted LEDs on the side of the plastic strobe at 2 to 4 Hz. The lens system diffuses the light to shine on the finger’s surface, revealing details of the fingerprint. Note that the imager is not directly under the finger. If it were, the sensor would either have to be the size of the fingerprint or the sensing module would have to be thicker to allow macro focusing of the image onto a smaller silicon area. Identix packages Motorola’s silicon with lens-

Figure 1

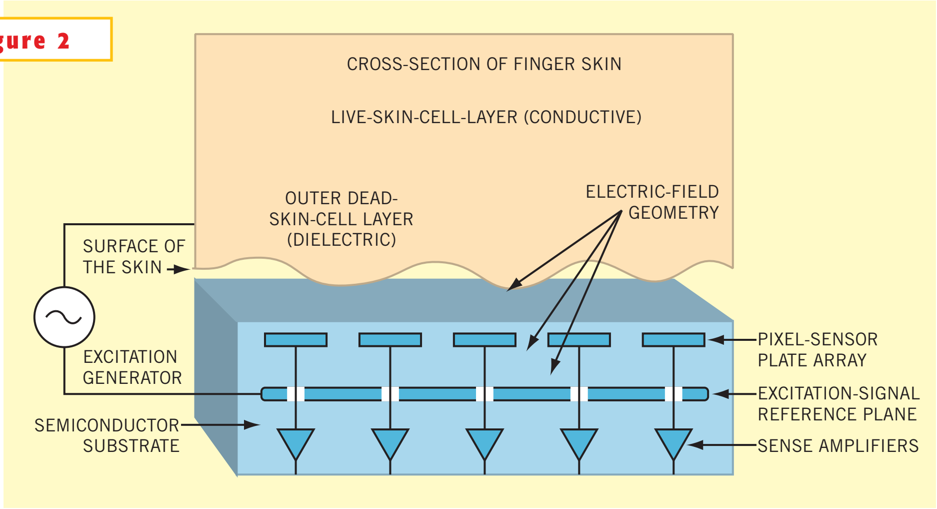


With a capacitive scanner, an air dielectric layer with variable thickness based on the valleys and ridges of a finger’s surface modulates the effective capacitance.

es and LEDs in a module. Light from the LEDs floods the underside of the finger sensor. Using the principles of frustrated internal refraction (FIR), the light is either reflected normally where there is no finger ridge on the surface (appearing light) or is reflected at a different angle (appearing dark). The image from the sensor is then reflected off a mirror, passed through a lens system, and focused onto the top of the assembly where the CMOS imager sits.

The imager, collecting as many as 12 frames/sec, makes a progressive scan of the array (320×590 pixels) and determines the window of interest (the location of the fingerprint). The ratio of reduction takes a 20×30-mm image down to 3×4 mm. Some advantages of this technique are that a user need not actually contact the silicon scanner. Although a guard ring can help diffuse ESD, as the plastic coating wears with use, ESD can become more of an issue. Additionally, given different lenses, the silicon sensor can continue to shrink in size and thus cost; it is not limited by the size of a fingerprint.

Figure 2


CROSS-SECTION OF FINGER SKIN
LIVE-SKIN-CELL-LAYER (CONDUCTIVE)
OUTER DEAD-SKIN-CELL LAYER (DIELECTRIC)
ELECTRIC-FIELD GEOMETRY
SURFACE OF THE SKIN
EXCITATION GENERATOR
SEMICONDUCTOR SUBSTRATE
PIXEL-SENSOR PLATE ARRAY
EXCITATION-SIGNAL REFERENCE PLANE
SENSE AMPLIFIERS

E-field scanners drive a signal through the conductive fluid layer of saline solution between the living and dead layers of skin. The layer of saline has the same shape as the external fingerprint. An array of antennas above the reference (bottom) plate then samples the electric field.

CAPACITIVE SCANNERS

An example of a capacitive scanner is the TouchChip Silicon Fingerprint Sensor from STMicroelectronics. Each of the sensor's pixel cells has a high-gain inverter connected to two adjacent top-metal plates separated from the skin's surface by a protective coating (**Figure 1**). Connecting the inverter input to one of the top metal plates and connecting an amplifier output to the other create a charge integrator. The integrator's feedback characteristic is the effective capacitance between the two metal plates. The finger on the sensor acts as a third plate separated from the metal plates by an air dielectric layer with variable thickness based on the valleys and ridges of the finger's surface; it modulates the effective capacitance. Adjacent cells in the array measure capacitance, and you can read it in a random-access mode.

E-FIELD SCANNERS

Authentec offers an e-field scanner that looks at the subsurface of the skin, past the dead portion and dirt, to the live layer of the skin. The e-field scanner works from the principle that two charged, parallel metal plates generate an electric field between them (**Figure 2**). If you change the shape of the top plate to be corrugated (like the ridges and valleys of a fingerprint), the field strength also changes with a modulation based on the shape of the top plate. Authentec's scanner uses the finger as the top plate and drives a signal through the finger. Under the dead layer of skin is a highly conductive fluid layer of saline solution, which cells produce when they die and burst. Outside the sensor is a conductive ring. When the finger touches the ring, it sends a signal through the finger and this conductive layer, which has the same shape as the external fingerprint. An array of antennas above the reference (bottom) plate then samples the e-field. The sensor then passes this digital representation of the e-field the host processor to be reconstructed into a gray-scale fingerprint image.

An advantage of e-field scanners is that they can read through most materials on the surface of the finger. For example, a wet or dirty finger cannot completely obliterate the electrical characteristic of the saline signal. Because the input signal can make the field stronger, the plastic coating protecting the scanner can be thicker than it is on other kinds of scanners. Additionally, e-field scanners can read worn-off or otherwise-damaged fingerprints.

PRINT PROCESSING

Typically, a sensor collects data at several frames per second. At this stage, the sensor adjusts itself, depending upon environmental factors, such as climate, humidity, and damaged fingerprints, that affect image quality. For example, people who work with their hands wear down their fingerprints, making them more difficult to capture. The scanner automatically optimizes various settings, such as gain, contrast, frequency, or phase shift, depending upon the sensor technology, to improve the quality of the captured image. Then, it captures the print that it will analyze. All this activity takes place within several hundred milliseconds.

Several stages of processing occur once you capture image. First, you must condense the digitized image into a more manageable format; that is, storing more than 150,000 pixels would require obscene amounts of memory and would make identification—comparing prints—computationally infeasible. A common method that the FBI uses identifies minutiae—details such as end ridges or bifurcations—and takes as many as 40 points to create a person's unique signature template. A fingerprint now requires about 128 bytes (**Figure 3**).

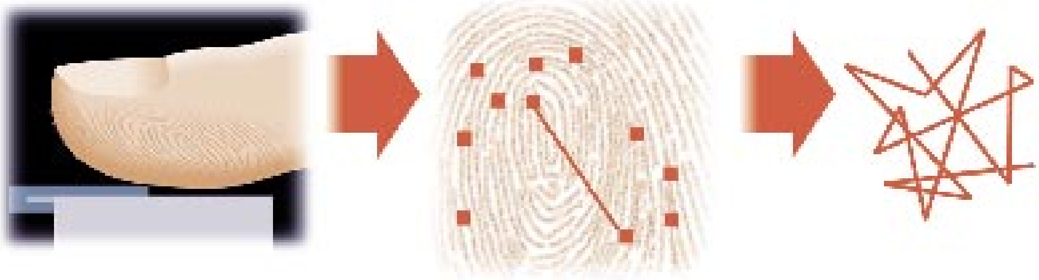
The second stage is to identify the fingerprint from a database. Each sensor vendor uses various proprietary algorithms, but the basic process is to compare templates and look for a best match. Because of the varying conditions under which they are captured, images do not perfectly match the minutiae characteristics saved in the database for each person who is to be recognized. Therefore, each algorithm usually has a parameterized tolerance for error that allows you to set the level of security.

Security is measured as false accepts and false rejects. A false accept is when a system recognizes a person's fingerprint it shouldn't have or when it recognizes the fingerprint as belonging the wrong person. A false reject is when a system rejects a valid fingerprint. The fewer the false accepts, the greater the number of false rejects. This relationship occurs because, to prevent false accepts, you must tighten tolerances, and captured images must more closely match the saved signature template in the database. The tightened tolerances, however, tend to cause the system to fail to recognize valid prints.

The false-accept/false-reject ratio determines the critical trade-off between security and ease of use. For example, a secure system may never falsely accept someone, but having such a high tolerance requires that the system capture valid prints several times before it accepts them. Although running your finger across the sensor 15 times may be acceptable in a top-secret government installation, consumers trying to use their credit cards to buy gas simply won't tolerate the inconvenience. Additionally, both time of day and other factors directly affect false rejects. A machinist with most of his or her prints rubbed off is likely to fail under highly secure settings. If such a person can't get past the front door because of the sensor, the sensor becomes a liability. Thus, important factors are not only how accurately a system can recognize fingerprints, but also how reliably it can capture that print. (For example, can the system obtain an image from every person?) More than one company has fallen victim to the trap of evaluating a fingerprint system using employees in the workplace cafeteria, whose demographic is typically 18- to 45-year-old men who tend to be clean and don't do much physical work to wear down their prints. The company determines that its system works reliably; then, when it receives the "street test," using a more reasonable statistical representation of the population, the system performs much worse than expected.

It's important to note that the false-accept/false-reject ratios are factors of both the recognition algorithms and the images themselves. Certainly, poorly captured images yield poor recognition results, but different algorithms yield different results even with the same captured images. These recog-

Figure 3



After a system captures a print image, a host processor extracts minutiae and then creates a template showing the geometric relationship between the minutiae. This process reduces a fingerprint image from more than 150,000 pixels to around 128 bytes.

nition ratios depend on the whole system. A vendor may be tempted to give ratios based solely on the algorithm using only clean images instead of the quality of images the sensor tends to capture. Additionally, vendors may not include "failures to acquire," that is, failed attempts to capture a print in their figures.

Finally, most fingerprint-image processing takes place on a host processor to keep down the cost of the scanner. This method also makes sense from the perspective of recognition; trying to connect a sensor to a potentially vast fingerprint database simply makes no sense. A final consideration for a fingerprint system is the secure transfer of the image to the processing platform. First, the bus passing the data must be wide enough to do so in a timely fashion, such as over a parallel or USB port. Second, because the bus is external and someone could conceivably compromise it, the system must send the image with encryption to both prevent someone from forcing a print into the system and prevent someone from lifting a valid print and using it later.□

You can reach Technical Editor Nicholas Cravotta at 1-510-558-8906, fax 1-510-558-8914, e-mail ednnick@pacbell.net.

FOR MORE INFORMATION...

For more information on products such as those discussed in this article, enter the appropriate numbers at www.ednmag.com/infoaccess.asp. When you contact any of the following manufacturers directly, please let them know you read about their products in *EDN*.

Authentec
1-321-308-1300
www.authentec.com
Enter No. 432

Identix
1-408-731-2000
www.identix.com
Enter No. 433

Motorola
1-480-814-3971
mot-sps.com/adc/Image_Capture/bio.html
Enter No. 434

STMicroelectronics
www.st.com
Enter No. 435

Veridicom
1-408-565-6000
www.veridicom.com
Enter No. 436

SUPER NUMBER

For more information on the products available from all of the vendors listed in this box, enter No. 437 at www.ednmag.com/infoaccess.asp.