How Fingerprint Scanners Work

by Tom Harris

Computerized fingerprint scanners have been a mainstay of spy thrillers for decades, but up until recently, they were pretty exotic technology in the real world. In the past few years, however, scanners have started popping up all over the place -- in police stations, high-security buildings and even on PC keyboards. You can pick up a personal USB fingerprint scanner for less than $100, and just like that, your computer's guarded by high-tech biometrics. Instead of, or in addition to, a password, you need your distinctive print to gain access.

Photo courtesy Siemens

A computer mouse with a built-in fingerprint scanner

In this article, we'll examine the secrets behind this exciting development in law enforcement and identity security. We'll also see how fingerprint scanner security systems stack up to conventional password and identity card systems, and find out how they can fail.

Fingerprint Basics

Fingerprints are one of those bizarre twists of nature. Human beings happen to have built-in, easily accessible identity cards. You have a unique design, which represents you alone, literally at your fingertips. How did this happen?

People have tiny ridges of skin on their fingers because this particular adaptation was extremely advantageous to the ancestors of the human species. The pattern of ridges and "valleys" on fingers make it easier for the hands to grip things, in the same way a rubber tread pattern helps a tire grip the road.

The other function of fingerprints is a total coincidence. Like everything in the human body, these ridges form through a combination of genetic and environmental factors. The genetic code in DNA gives general orders on the way skin should form in a developing fetus, but the specific way it forms is a result of random events. The exact position of the fetus in the womb at a particular moment and the exact composition and density of surrounding amniotic fluid decides how every individual ridge will form.

So, in addition to the countless things that go into deciding your genetic make-up in the first

place, there are innumerable environmental factors influencing the formation of the fingers. Just like the weather conditions that form clouds or the coastline of a beach, the entire development process is so chaotic that, in the entire course of human history, there is virtually no chance of the same exact pattern forming twice.

Consequently, fingerprints are a unique marker for a person, even an identical twin. And while two prints may look basically the same at a glance, a trained investigator or an advanced piece of software can pick out clear, defined differences.

This is the basic idea of fingerprint analysis, in both crime investigation and security. A fingerprint scanner's job is to take the place of a human analyst by collecting a print sample and comparing it to other samples on record. In the next few sections, we'll find out how scanners do this.

Optical Scanner

A fingerprint scanner system has two basic jobs -- it needs to get an image of your finger, and it needs to determine whether the pattern of ridges and valleys in this image matches the pattern of ridges and valleys in pre-scanned images.

There are a number of different ways to get an image of somebody's finger. The most common methods today are **optical scanning** and **capacitance scanning**. Both types come up with the same sort of image, but they go about it in completely different ways.

The heart of an optical scanner is a **charge coupled device** (CCD), the same light sensor system used in digital cameras and camcorders. A CCD is simply an array of light-sensitive diodes called **photosites**, which generate an electrical signal in response to light photons. Each photosite records a pixel, a tiny dot representing the light that hit that spot. Collectively, the light and dark pixels form an image of the scanned scene (a finger, for example). Typically, an analog-to-digital converter in the scanner system processes the analog electrical signal to generate a digital representation of this image. See How Digital Cameras Work for details on CCDs and digital conversion.

The scanning process starts when you place your finger on a glass plate, and a CCD camera takes a picture. The scanner has its own light source, typically an array of light-emitting diodes, to illuminate the ridges of the finger. The CCD system actually generates an **inverted image** of the finger, with darker areas representing more reflected light (the ridges of the finger) and lighter areas representing less reflected light (the valleys between the ridges).

Before comparing the print to stored data, the scanner processor makes sure the CCD has captured a clear image. It checks the average pixel darkness, or the overall values in a small sample, and rejects the scan if the overall image is too dark or too light. If the image is rejected, the scanner adjusts the exposure time to let in more or less light, and then tries the scan again.

If the darkness level is adequate, the scanner system goes on to check the **image definition** (how sharp the fingerprint scan is). The processor looks at several straight lines moving horizontally and vertically across the image. If the fingerprint image has good definition, a line running perpendicular to the ridges will be made up of alternating sections of very dark pixels and very light pixels.

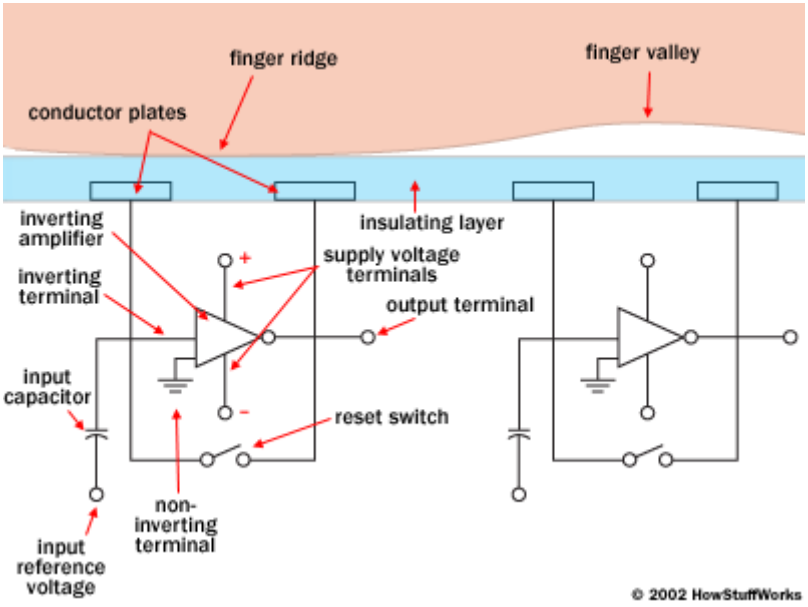
If the processor finds that the image is crisp and properly exposed, it proceeds to comparing the captured fingerprint with fingerprints on file. We'll look at this process in a minute, but first we'll examine the other major scanning technology, the **capacitive scanner**.

Capacitance Scanner

Like optical scanners, capacitive fingerprint scanners generate an image of the ridges and valleys

that make up a fingerprint. But instead of sensing the print using light, the capacitors use electrical current.

The diagram below shows a simple capacitive sensor. The sensor is made up of one or more semiconductor chips containing an array of tiny **cells**. Each cell includes two **conductor plates**, covered with an insulating layer. The cells are tiny -- smaller than the width of one ridge on a finger.



The sensor is connected to an **integrator**, an electrical circuit built around an **inverting operational amplifier**. The inverting amplifier is a complex semiconductor device, made up of a number of transistors, resistors and capacitors. The details of its operation would fill an entire article by itself, but here we can get a general sense of what it does in a capacitance scanner. (Check out this page on operational amplifiers for a technical overview.)

Like any amplifier, an inverting amplifier alters one current based on fluctuations in another current (see How Amplifiers Work for more information). Specifically, the inverting amplifier alters a supply voltage. The alteration is based on the relative voltage of two inputs, called the inverting terminal and the non-inverting terminal. In this case, the non-inverting terminal is connected to ground, and the inverting terminal is connected to a reference voltage supply and a **feedback loop**. The feedback loop, which is also connected to the amplifier output, includes the two conductor plates.

As you may have recognized, the two conductor plates form a basic capacitor, an electrical component that can store up charge (see How Capacitors Work for details). The surface of the finger acts as a third capacitor plate, separated by the insulating layers in the cell structure and, in the case of the fingerprint valleys, a pocket of air. Varying the distance between the capacitor plates (by moving the finger closer or farther away from the conducting plates) changes the total capacitance (ability to store charge) of the capacitor. Because of this quality, the capacitor in a cell under a ridge will have a greater capacitance than the capacitor in a cell under a valley.

To scan the finger, the processor first closes the reset switch for each cell, which shorts each amplifier's input and output to "balance" the integrator circuit. When the switch is opened again, and the processor applies a fixed charge to the integrator circuit, the capacitors charge up. The capacitance of the feedback loop's capacitor affects the voltage at the amplifier's input, which affects the amplifier's output. Since the distance to the finger alters capacitance, a finger ridge will result in a different voltage output than a finger valley.

The scanner processor reads this voltage output and determines whether it is characteristic of a ridge or a valley. By reading every cell in the sensor array, the processor can put together an overall picture of the fingerprint, similar to the image captured by an optical scanner.

The main advantage of a capacitive scanner is that it requires a real fingerprint-type shape, rather than the pattern of light and dark that makes up the visual impression of a fingerprint. This makes the system harder to trick. Additionally, since they use a semiconductor chip rather than a CCD unit, capacitive scanners tend to be more compact that optical devices.

Analysis

In movies and TV shows, automated fingerprint analyzers typically overlay various fingerprint images to find a match. In actuality, this isn't a particularly practical way to compare fingerprints. Smudging can make two images of the same print look pretty different, so you're rarely going to get a perfect image overlay. Additionally, using the entire fingerprint image in comparative analysis uses a lot of processing power, and it also makes it easier for somebody to steal the print data.

Instead, most fingerprint scanner systems compare specific features of the fingerprint, generally known as **minutiae**. Typically, human and computer investigators concentrate on points where ridge lines end or where one ridge splits into two (**bifurcations**). Collectively, these and other distinctive features are sometimes called **typica**.

The scanner system software uses highly complex algorithms to recognize and analyze these minutiae. The basic idea is to measure the relative positions of minutiae, in the same sort of way you might recognize a part of the sky by the relative positions of stars. A simple way to think of it is to consider the shapes that various minutia form when you draw straight lines between them. If two prints have three ridge endings and two bifurcations, forming the same shape with the same dimensions, there's a high likelihood they're from the same print.

To get a match, the scanner system doesn't have to find the entire pattern of minutiae both in the sample and in the print on record, it simply has to find a sufficient number of minutiae patterns that the two prints have in common. The exact number varies according to the scanner programming.

Pros and Cons

There are several ways a security system can verify that somebody is an authorized user. Most systems are looking for one or more of the following:

- What you have
- What you know
- Who you are

To get past a "what you have" system, you need some sort of "token," such as an identity card with a magnetic strip. A "what you know" system requires you to enter a password or PIN number. A "who you are" system is actually looking for physical evidence that you are who you say you are -- a specific fingerprint, voice or iris pattern.

"Who you are" systems like fingerprint scanners have a number of advantages over other systems. To name few:

- Physical attributes are much harder to fake than identity cards.
- You can't guess a fingerprint pattern like you can guess a password.
- You can't misplace your fingerprints, irises or voice like you can misplace an access card.
- You can't forget your fingerprints like you can forget a password.

But, as effective as they are, they certainly aren't infallible, and they do have major disadvantages. Optical scanners can't always distinguish between a picture of a finger and the finger itself, and capacitive scanners can sometimes be fooled by a mold of a person's finger. If somebody did gain access to an authorized user's prints, the person could trick the scanner. In a worst-case scenario, a criminal could even cut off somebody's finger to get past a scanner security system. Some scanners have additional pulse and heat sensors to verify that the finger is alive, rather than a mold or dismembered digit, but even these systems can be fooled by a gelatin print mold over a real finger. (This site explains various ways somebody might trick a scanner.)

To make these security systems more reliable, it's a good idea to combine the biometric analysis with a conventional means of identification, such as a password (in the same way an ATM requires a bank card and a PIN code).

The real problem with biometric security systems is the extent of the damage when somebody does manage to steal the identity information. If you lose your credit card or accidentally tell somebody your secret PIN number, you can always get a new card or change your code. But if somebody steals your fingerprints, you're pretty much out of luck for the rest of your life. You wouldn't be able to use your prints as a form of identification until you were absolutely sure all copies had been destroyed. There's no way to get new prints.

But even with this significant drawback, fingerprint scanners and biometric systems are an excellent means of identification. In the future, they'll most likely become an integral part of most peoples' everyday life, just like keys, ATM cards and passwords are today.