U.are.U®

Fingerprint Recognition System
Technology Overview &
Competitive Analysis

Introduction

This white paper provides an overview of the technical issues surrounding fingerprint capture and user authentication in real-world applications. We compare competing hardware and software technologies and highlight the superiority of DigitalPersona's integrated software, firmware and hardware solutions.

We compare technologies according to the following criteria:

- Image Capture/Hardware: Comparison of hardware technologies for obtaining the fingerprint image and transmitting it to the host.
- Image Capture/Firmware: Overview of the competitive advantages of the firmware inside DigitalPersona's intelligent image capture devices.
- Recognition Algorithms: Overview of the technology approach to fingerprint recognition created by DigitalPersona and the advantages of DigitalPersona's award-winning recognition algorithms over competing solutions.
- DigitalPersona Advantages: Overview of the company's leadership in user authentication technologies, commitment to IT security, and ability to provide complete, integrated user authentication solutions.

Competitive Features of U.are.U Image Capture Hardware

Overview

Two major thrusts currently exist in image capture technology for mass-market fingerprint recognition devices: optical and solid-state capacitive. DigitalPersona fingerprint recognition software works with both optical and solid state technologies. The company has selected an optimized version of optical technology for its U.are.U product line. This document compares the advantages of each hardware approach and explains why our optical technology makes the most sense in today's market for use in both embedded and standalone applications.

Optical versus Solid State/Capacitive Technologies

DigitalPersona analyzed currently available hardware solutions and concluded that, while solid-state technology can be an acceptable alternative for applications where overall thickness of components is the single overriding concern, it is inferior for mass-market fingerprint capture products. This document analyzes fingerprint capture hardware in terms of suitability for real-world applications, component size, suitability for embedded applications, image quality, and cost. It also highlights the unique features of DigitalPersona's award-winning intelligent-sensor technology and explains why it outperforms the competition.

Reliability

Reliability is particularly crucial in fingerprint recognition hardware. DigitalPersona has studied the performance characteristics of optical and solid state hardware and has concluded that optical technology is more reliable over time. Reliability factors include:

- Susceptibility of the surface window to damage from objects being dropped on it.
- Wear and tear on the sensor window surface over time
- Susceptibility to electrostatic discharge and other electrical noise
- Contamination from dirt

Fragility

When DigitalPersona considered technology directions available it looked to other mass-market input devices. Optical components have been used in computer mice and desktop scanners for many years and in those products they have proven to be extremely reliable. DigitalPersona believes fingerprint recognition hardware components must have a similar level of durability.

Based on in-depth, long-term experience with computer input devices, the company believes that optical technology is highly stable under conditions of day-to-day wear. U.are.U has the added advantage of having been proven in the retail marketplace where the product has been used over a prolonged period in a widely varied market.

U.are.U has proven itself reliable for its customer base over a prolonged period beginning with its introduction in August 1998.

Durability of Sensor Window Surface

It is a known fact that silicon is not meant to be touched. Capacitive sensors require that the user put his or her finger directly onto a piece of silicon day after day. While capacitive sensors can be coated to protect against abrasion, this coating is subject to wear and scratches easily. A solid state sensor cannot sustain the drop of a ballpoint pen onto its surface from a height of one foot while the optical sensor has no trouble with such a test. Moreover, silicon sensors have not yet been proven in real-world applications while optical technology is proven.

DigitalPersona's U.are.U sensor window is durable and not subject to scratching. The company provides an added coating over its sensor window to improve performance with certain fingerprints.

Susceptibility to Electro-Static Discharge (ESD)

DigitalPersona has not implemented a surface capacitive solution for its U.are.U product line specifically because of the ESD problems that these solid state components have exhibited. It is a well-known problem that an ESD discharge can permanently destroy the circuitry of a silicon sensor. Major OEM customers require fingerprint components to withstand ESD ratings of 10KV of electricity. Capacitive technologies typically can withstand no more than a 1KV discharge. A user walking across a carpet in winter can easily build up a charge of 10KV. Silicon sensors have not yet demonstrated an ability to withstand such a discharge. This means that a user can cause a solid state unit to fail at any time just by touching it with a finger.

Capacitive solutions are especially susceptible to ESD problems because their electrical circuits are particularly close to the sensor surface – less than a fraction of a millimeter. Tiny openings in the surface allow electricity to get into the unit and damage the elements. Some providers try to resolve the ESD problem by putting a mechanical metal door over the sensor surface. As users push back the door with their finger, the door accepts the electrical charge and the circuitry is spared. This solution, along with others designed to mitigate ESD problems on capacitive technologies, seems to DigitalPersona to be unacceptable. The sprint-loaded door solution is inconvenient for the user and often causes faulty positioning of the fingerprint on the device. Failure of the door over time makes the fingerprint sensor unworkable.

DigitalPersona's U.are.U sensor components withstand an electrical discharge of over 15KV with no performance failure. The plastic cover and case around the U.are.U components provide full protection from ESD.

Dirt Contamination/Wear and Tear

DigitalPersona's U.are.U product line has withstood the rigors of the retail marketplace with customers using the product in highly "contaminated" environments from auto repair shops to standard office settings. While it is always the case that extreme dirt conditions will compromise performance over time, DigitalPersona believes that the optical components the company has adopted for the U.are.U line are far more likely to perform well over time. The surfaces and case of the U.are.U device protect the internal components from wear, and any accumulations of dirt on the sensor window are easily removed.

Size

For embedded fingerprint recognition solutions there are two critical size criteria:

- size of the sensor window
- overall thickness of the components.

Capacitive hardware providers seek to reduce the cost of their sensor components by reducing the size of the sensor window. DigitalPersona believes that when using a flat sensor window the size of that window must be dictated by the average size of the fingerprint – approximately 12mm by 18mm. Reducing the size to be smaller than the fingerprint compromises performance in the following ways:

- The sensor does not capture the entire fingerprint, recognition is based on a small amount of data, and false acceptance and rejection rates increase.
- Users must "line up" their fingers precisely on the sensor window, making the sensor more difficult and awkward to use and increasing the potential for errors.

When considering fingerprint capture hardware for embedded solutions, inside a keyboard, laptop or other product, thickness of components becomes a crucial issue. DigitalPersona's new fingerprint sensors for embedded applications are approximately 1mm thicker than typical silicon sensors. DigitalPersona believes that the poor performance and poor reliability of capacitive products currently available makes them an inferior choice for embedded solutions despite their slightly thinner profile.

Image Quality

Those new to issues surrounding fingerprint recognition often assume that the greatest difficulty in obtaining a satisfactory fingerprint image is moisture. In fact the opposite is true. The most difficult fingerprint to image is a dry print. This is because it is more difficult to make the ridges on a dry print sit flush on the sensor surface. Tiny areas of the ridge surface remain out of contact with the sensor, and the result is a poor image.

The surface of capacitive sensors is hard, making is especially difficult to obtain a satisfactory image from a dry fingerprint. The user must place his finger directly on the sensor surface, which cannot conform to the ridges of a dry finger. The finger does not remain on the sensor surface long enough for heat from the sensor to warm the print, and obviate the dry finger problem by causing the print to "settle" onto the hard surface, as some capacitive sensor vendors claim.

DigitalPersona has added a thin, tough silicone coating to the sensor window of its devices to ensure that an optimal fingerprint image is always obtained. The conformal silicone coating creates a superior optical interference between the imaging window and the fingerprint ridges of either dry or moist skin. Such a solution cannot be adopted for use with capacitive sensors and these sensors have less ability to recognize dry fingerprints.

Cost

When DigitalPersona considers cost of components it looks not just to the cost of components today but to the cost of components as volumes increase – at the potential for cost reduction. Processed silicon chips are a commodity with standard pricing. Therefore, the cost of silicon sensors is also not expected to go down significantly.

Capacitive sensors are costly due to the requirement for a large silicon area and the accompanying yield problems. The silicon imagers in DigitalPersona's optical sensors are significantly smaller and less costly than that of a capacitive sensor. The silicon imager on a capacitive sensor has to be at least as large as the image capture area. In an optical sensor the optics reduce the fingerprint image down, in most cases reducing the size requirement for the silicon imager by a factor of 10.

As unit volumes increase, the potential for cost reduction on the U.are.U optical components is higher than the potential on solid state solutions. Looking to the digital camera market, it is clear that optical technology in high volume leads directly to lower unit costs. With silicon solutions even in extremely high volume, the cost of silicon is fixed, and the cost of manufacturing is high.

DigitalPersona's optical technology uses inexpensive off-the-shelf sensor arrays and LED light sources. DigitalPersona sensors use the same imager chip technology that goes into PC cameras: a high volume, mature technology that provides significant cost and reliability benefits. The optical design of the U.are.U product achieves high image quality with the use of low cost lenses and plastic components.

Competitive Features of U.are.U Firmware

Overview

Part of the reason for the superior recognition capabilities of the U.are.U system is the firmware inside all U.are.U intelligent sensors. This firmware is unique to DigitalPersona and gives all U.are.U products competitive advantage in the timing of the image capture – typically one tenth of one second. It also provides the ability to distinguish a fake fingerprint, establishment of a secure link with the host system, and ability to offload processing requirements from the host.

Fake-Finger Detection

U.are.U hardware and firmware acting together make it virtually impossible to breach the system and obtain acceptance based on a fake fingerprint. The system will not accept a 2D image, either on transparent film or on paper, and it is able to detect virtually all 3D molds of fingerprints. While no fingerprint recognition device is 100% secure from a highly focused attempt with the most sophisticated tools, U.are.U firmware makes the possibility of such a breach remote.

AutoCapture

AutoCapture is an important factor in obtaining the best possible fingerprint image. The U.are.U sensor scans for the presence of a fingerprint at a rate of 30 times a second. As a fingerprint comes to rest on the sensor window, the firmware is able to detect the precise optimal moment when the print image should be captured. If the image is captured too soon only part of the finger would be resting on the sensor window and important data would be lost. If the image is captured too late the finger would be pressing too hard on the window and the image would be compromised. AutoCapture ensures that the maximum amount of data is available upon which to base recognition.

After the user quickly taps his finger on U.are.U, the Sensor sends a single, compressed image to the host processor. Less-sophisticated systems require the user to hold his finger on the sensor window while the non-intelligent sensor sends a slow video stream of images to the PC.

Challenge-Response Link

U.are.U ensures that the link with the host system is secure. One element of this secure relationship is the ability of the firmware to establish a challenge-response link between the sensor and the host.

When the intelligent U.are.U sensor captures a fingerprint, it interrupts the host to notify it that a fingerprint template is ready to be sent. In response, the host generates a random number that it sends back to the sensor. The random number is used once and only once. The sensor incorporates the number into the encrypted data that is transmitted back to the host. The host will only accept data from the sensor that was encrypted using the particular random number it encrypted using the

particular random number it has just sent. The challenge-response link prevents "replay attacks" in which spurious data is sent across the wire to the host. Furthermore, the fingerprint image data is encrypted, so no one can read a user's fingerprint or insert false fingerprint data into the information that is sent to the host.

When used on a network in which Windows 95/98 is running on the client, U.are.U establishes a challenge-response link between the sensor and the NT server. The un-secure Windows 95/98 client is used as a pass-through, and overall security is maintained throughout.

Latent Image Removal

Each time a finger is placed on the sensor window, a smudge remains as an after-image on the window surface. If this "latent image" were not detected and removed by the sensor it could be incorporated into the subsequent fingerprint scan and could lead to false acceptance or rejection.

The U.are.U firmware is able to automatically compensate for latent fingerprints, removing them from the data that is collected from subsequent scans. This feature significantly improves recognition results, especially on systems that are used by more than one person.

USB Format and Interface Control

DigitalPersona Sensors send only encrypted fingerprint data to the host, and they format the encrypted fingerprint image for transmission over a high speed Universal Serial Bus (USB) interface before sending it. Unlike competing products which transmit images in the clear, the DigitalPersona Sensor sends only encrypted, time stamped data, ensuring that the interface between the Sensor and the host is fully secure.

Host Interrupt

A number of DigitalPersona's competitors provide unintelligent sensors that require constant polling by the host system. Many of these devices send a continuous stream of video images to the host and it is up to the host to process them continuously, determining when a fingerprint image has come across the line. These images are sent across in the clear without the security of encryption, and with no steps taken to maintain security. U.are.U generates an interrupt when it is ready to transmit fingerprint data. The sensor interrupts the host only when it is ready to transmit a complete fingerprint template for recognition, offloading the host and maintaining a secure link.

U.are.U Recognition Engine Competitive Features

DigitalPersona's recognition engine has won numerous awards in competitive reviews and analyst reports, and was selected as the editor's choice from both PC Magazine and Network Computing Magazine. In every competitive review DigialPersona's U.are.U is cited for its superior recognition capabilities. Testimonial from such reviews includes:

- "Recognized each of us instantly without a mistake. Keeps PCs secure."
  Fortune Magazine, 5/24/99
- "U.are.U performed without fail during testing…Recognized users with exceptional accuracy and speed….We weren't able to fool it in our labs."
  PC Magazine, 2/23/99
- "Faster than any other device we tested."
  Network Computing Magazine, 6/1/98

Continuously Improved

While the U.are.U hardware, firmware and applications all contribute to superior results, the U.are.U Recognition Engine is in large part responsible for the fast, accurate recognition of the U.are.U system. This engine was first developed a number of years ago and has been continuously improved ever since.

Developed for the IS Market and Real-World Application

As with all DigitalPersona technology, the Recognition Engine has been optimized for real-world application, meaning that it can be used by a wide variety of people under widely varied environmental conditions with no outside assistance or supervision. The Recognition Engine has met the challenge of real-world variability and continues to out-perform the competition.

As an example, the U.are.U Engine is 100% rotation invariant, meaning that it will recognize a print from any angle. While competing products are now struggling to meet this challenge as well, only the U.are.U Engine provides time-tested rotation invariance. A further example of the company's commitment to the real world is AutoCentering. Many competing products require that users precisely line up their fingerprint on the sensor window with the sensor not working unless the fingerprint is centered on a crosshair. DigitalPersona's Engine takes real-world issues into account and automatically compensates when users' prints are not lined up in the center of the sensor window.

A further strength of the U.are.U Engine for use in the computer market is that it has been developed specifically for this market. Competing products were originally developed for the law enforcement or forensics markets in which providing a fingerprint image was an attended or supervised process. In those markets an attendant placed the fingerprint onto the sensing area, lining it up properly and ensuring that the fingerprint image was optimized. The engines developed for these attended process markets then had to be adapted for the unattended model of the current market.

Data Analysis

The greatest strength of the U.are.U Engine is the amount of data and the types of data that it includes in the process of recognition. Fingerprints contain a tremendous amount of data – enough to establish the identity of each of us with an extremely high degree of certainty. Certain fingerprint recognition engines consider only a small portion of that data in authenticating users. While these engines might recognize one type of fingerprint they might have trouble with another, or they might provide a high number of false acceptance or rejections. The U.are.U Recognition Engine looks at both a large amount of data and at different types of data to establish a match.

The U.are.U Engine analyzes three types of fingerprint information:

- Global Features, such as pattern area, core point, type lines, delta, and ridge count
- Ridge Orientation, including the basic ridge patterns and orientation
- Minutia, including type, orientation, spatial frequency, curvature, and position of ridge endings and bifurcations.

DigitalPersona does not disclose the proprietary methodology it uses to analyze amount and types of fingerprint data. However, the company stands behind its Recognition Engine as the fastest and most accurate in the world for use in the IS market.

Optical versus Capacitive Fingerprint Sensor Technology

Feature	DigitalPersona: Optical	Capacitive
Image Area	Large and convenient (15mm x 20mm)	Small and expensive (10mm x 10mm)
Fake Finger Detection	Difficult to fool	Easily fooled
Design Maturity	Hundreds of thousands in daily use	New
ESD Resistance	Withstands 15KV	Withstands 1KV
Water Resistance	Resistant, sealed	Non-resistant. Can be ruined by water
Salts/Perspiration Effects	Resistant	May cause shorts, may corrode semiconductor surface
Protected Sensor Window	Sealed protective window	Unsealed. Direct contact w/semiconductor surface is required.
Manufacturing Lead Time	Short, predictable	Long
Manufacturing Yield	Excellent	Complicated fab process lowers yield
Sensor Window Impact Resistance	Durable plastic window	Fragile crystal surface. Dropping pencil on window fractures surface.
Ability to Image all Fingerprints	Yes	Difficulty w/dry and wet prints – normal only
Special Coating to Aid Dry Print Image Capture	Yes	Not possible
Susceptible to Cost Reduction	Highly susceptible to cost reduction as component volumes increase	Not Susceptible to cost reduction. Silicon cannot be reduced below size of print