PERGAMON

Pattern Recognition 36 (2003) 361–369

PATTERN RECOGNITION
THE JOURNAL OF THE PATTERN RECOGNITION SOCIETY

www.elsevier.com/locate/patcog

Innovations in fingerprint capture devices

Xiongwu Xia*, Lawrence O'Gorman

Veridicom Inc. 31 Scotto Pl, Dayton, NJ 08810, USA

Received 21 December 2001

Abstract

The image capture device plays a key role in fingerprint authentication. In recent years, we have seen remarkable innovations in these devices, which have reduced the size, lowered the price, and improved the performance. These new sensors have paved the way for deployment of fingerprint authentication beyond law enforcement applications to more widespread personal authentication. This paper provides an overview of fingerprint capture devices. Sensor issues and future trends are also discussed.

Keywords: Fingerprint capture device; Authentication; Optical sensor; Solid-state sensor

1. Introduction

Biometrics offers to replace or complement passwords to offer a higher level of user convenience and network security. Fingerprint, voice, iris, and face comprise the most prevalent modalities of effective biometrics for computer security [1]. No matter what kind of biometric, there is always a biometric capture device, and it is the predominant factor of system price and verification performance for the complete system.

Inking is the traditional ways of fingerprint capture, which has a long history and is still being used by some law enforcement applications. But it is inconvenient and time consuming due to the subsequent digitization. On the contrary, the live scan fingerprint device can capture a digital fingerprint image in real time.

There are three types of live scan devices: optical, solid-state and other [2]. Optical fingerprint capture devices use a light source and lens to image the fingerprint. The image is captured by a CCD/CMOS camera. Solid-state sensors appeared on the market in the mid-1990s. These sensors comprise an array of sensing elements that image the fingerprint via different technologies. Usually the solid-state sensors have on-chip A/D (analog to digital converter) so that a digital image can be generated. The third category, "other", includes devices that employ ultrasonic means for image capture [3].

One occasional problem in fingerprint systems is the poor image quality. Fingerprint quality not only varies widely, but also changes over time. Elderly persons or manual workers tend to have poorer fingerprints. Even the same finger can be different due to skin condition, weather conditions and finger cuts [4]. Since the quality and condition of human fingerprints are quite different, the image capture devices play a crucial role yielding a correct result for the authentication system. The ability to capture dry, wet, or other poor quality fingerprints becomes critical in commercial systems. Actually the image quality for the same person's finger can be quite different using different devices. The paper will discuss such issues and measurements for fingerprint sensors. Fig. 1 illustrates various finger conditions.

Low price, small size, and high recognition performance are the three challenges that must be met to achieve large deployment of a fingerprint device. Recent innovations for fingerprint capture devices have shown considerable progress toward lower cost, smaller size, and good recognition. It is these devices that have paved the way toward personal

* Corresponding author. Tel.: +1-732-829-2281; fax: +1-732-355-0106.

E-mail address: sam@veridicom.com (X. Xia).

0031-3203/02/$22.00
PII: S0031-3203(02)00036-5

Fig. 1. Images of various finger conditions: (a) normal finger; (b) dry finger; (c) wet finger; (d) poor quality finger.

authentication, where a fingerprint verification device is practical for any user of the internet, and for that matter a garage door or soda machine.

This paper examines innovations of fingerprint capture devices. Sensor issues are discussed in the next section. Section 3 describes the optical sensor. Section 4 describes the solid-state sensor. Summary and conclusions are in Section 5.

2. Sensor issues

Important factors to describe and compare fingerprint capture devices can be categorized as: cost, performance, and size [5]. We describe these below.

Cost: Cost is obviously an important factor. Fingerprint capture devices have fallen in price from about US$1500 to $30 since the early 1990s. We can expect further reduction of price with more technical innovations and with larger volume sales of the devices.

Performance: The performance includes various factors such as image resolution, bit depth, image quality, image capture area, and sensor durability.

The FBI image resolution standard for fingerprint is 500 dpi (dots per inch) [6]. Most commercial devices meet this requirement, however, some have lower resolutions down to 250 dpi. It is debatable what minimum resolution is sufficient for the population of users, however, it is understood that lower resolution may result in difficulty resolving ridges from valleys in fingerprints of people with narrow ridge spacing, and for children. Furthermore, some feature extraction algorithms require higher resolution, though specialized algorithms may deal with lower resolution well.

The FBI standard for pixel bit depth is 8 bits, which yields 256 levels of gray. Some sensors actually capture only 2 or 3 bits of real fingerprint information and then scale it to 8 bits. Thus the effective bit depth is 2–3, not 8. There is no definitive study that shows how recognition performance decreases when bit depth is decreased. However, it is understood that some degree of bit depth above 1 bit is necessary for good performance of many feature extraction algorithms.

Image quality is another key factor. Most sensors can handle "normal" finger quality well. But the ability to capture dry, wet, or poor quality fingerprints is more important in commercial applications. Some solid-state sensors have locally adjustable gain control. It enables automatic

Table 1
Comparison of fingerprint capture devices

Company	Technology	Type	Area (in)	System size	Resolution [dpi]	Bits/Pixel	Cost
Identicator	Optical	Touch	0.6×0.72	small	331	8	Low
Digital Persona	Optical	Touch	0.7×0.7	small	300	8	Low
SecuGen	Optical	Touch	0.53×0.64	small	450	8	Low
Ethentica	Electro-optical	Touch	0.56×0.76	small	400	8	Low
Veridicom	Capacitive	Touch	0.6×0.6	small	500	8	Low
Authentec	*E*-field	Touch	0.51×0.51	small	250	8	Low
Infineon	Capacitive	Touch	0.43×0.56	small	500	8	Low
Atmel	Thermal	Swipe	0.55×0.06	smaller	500	8	Lower
Veridicom	Capacitive	Swipe	0.51×0.1	smaller	500	8	Lower

adjustment of pixel gain to better image difficult fingers and difficult areas of a finger. This is discussed further in Section 4.

The FBI standard for image capture area is 1×1 in. This is sufficient area even for very large fingerprints. The larger the area of the finger that is captured, the more ridges and valleys are captured and the more distinctive the fingerprint is. Especially, for recent fingerprint capture devices for personal use, area is sacrificed to reduce cost and to fit into a smaller footprint. There is a very real tradeoff here between size and resulting recognition rate: the smaller the fingerprint area, the worse the recognition rate. An exception to this is the "swipe" sensor, which is much smaller than other sensors and requires the user to move (swipe) their fingerprint across its surface. This is described further in Section 4.

Sensor durability includes scratch-resistance, impact-resistance, impermeability to liquids, resistance to greasy residue buildup (latent image), and resistance to electro-static discharge (ESD). Older optical sensors meet these criteria well, since the glass surface (platen) upon which the finger is placed is quite durable. They should just be cleaned periodically. More recent optical sensors have plastic platens and special coatings to enhance image quality, both of which are susceptible to scratching and dirt buildup. Durability is more challenging for solid-state sensors. The first rule for an electronics engineer is to refrain from touching the silicon chip, however, fingerprint chips must be touched. Therefore, they must resist damage due to scratching, tapping with a sharp object, liquid permeability (in particular sodium chloride, which is corrosive and present in finger oils), and ESD at least above 8 kV (an industry minimum for most consumer electronics).

Size: The development of solid-state sensors brought the size reduction from what was brick-size for an optical device to postage size. Further integration on the chip has enabled even smaller system size with incorporation of A/D circuitry and bus circuitry onto the chip. The optical sensor has an inherent size limitation due to the required optical path length between platen and imager, and tradeoff between small focal length versus optical distortion from wide-angle lenses. However, optical readers have reduced substantially in size as well due to technological improvements as discussed in Section 3. For incorporation into a mobile device such as laptop computer or PDA, the chip has been favored so far due to its much thinner package. Optical and electro-optical devices as well as solid-state devices are small enough now to be incorporated into a keyboard or PCMCIA card [7].

Other Issues: There are other issues that must be considered when evaluating sensors. These include power consumption, I/O interface (USB, parallel port), operation environment (temperature, humidity), weight, and user population etc. Live finger detection can be a challenge task for sensors. Most sensors only take three dimension image and cannot be spoofed by a printed image.

It is best to perform a comparative test of devices in a similar environment to determine the most appropriate device for particular usage. Sensors are also designed to work best with the specific fingerprint matching algorithms. For instance, some matchers may work well for a lower resolution image while others may not. Software is also used to fix common hardware drawbacks such as latent fingerprints. So there is no absolute comparison rule for sensors and we have to evaluate sensor and software as a whole system. Table 1 summarizes features of some fingerprint capture devices that are commercially available [8].

3. Optical sensor

Before the introduction of optical sensors, fingerprints were mainly captured for law enforcement applications. In a traditional automatic fingerprint identification system (AFIS), a finger is inked, rolled onto paper, and digitized by a scanner. This system is expensive and time consuming, not to mention messy. The development of live scan

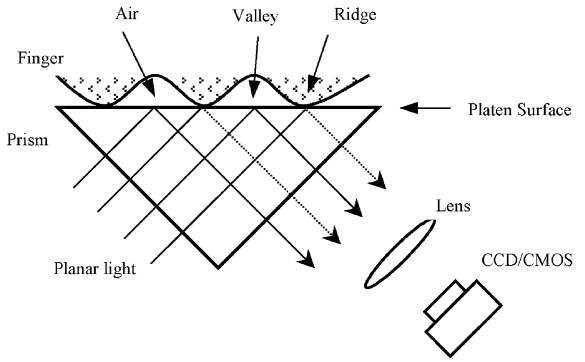

Fig. 2. Optical sensor.

devices obviated the need for inking since fingerprint is directly scanned.

3.1. Tradition optical sensor

Optical fingerprint capture is typically based on the frustrated total internal reflection (FTIR) phenomenon, as illustrated in Fig. 2 [9–11]. When a finger touches the platen, the refractive index is different between the ridge and valley. The light that passes through the glass upon valleys (air on the glass surface) is totally reflected. The light that passes through the glass upon ridges is not reflected. The reflected light is focused by a lens onto a CCD or CMOS [12] camera where the image is captured. Because, FTIR images a three-dimensional surface, optical sensor is not deceived by presentation of a photograph or printed image of a fingerprint.

Several recent innovations have improved the optical sensor design:

- CMOS camera versus CCD, the CMOS camera has an on-chip A/D that reduces the cost.
- Modular optical core design, this is usually a pre-molded plastic lens unit that assures accuracy of the optical path without calibration that was required with previous glass-lens designs.
- Improvements in optical components, such as film planar light, and prism protecting coat, as are described below.

CCD usually generates an analog video output, thus it needs a frame grabber card to convert the signal to a digital image. This makes it expensive and complicated for installation and maintenance. CMOS camera incorporates A/D conversion on-chip and lowers the cost and complexity of the system significantly.

Optical path, S, is defined as the total optical length between the finger surface and sensor array. Since the fingerprint size is fixed (a typical design has the finger 15 mm in width and 20 mm in height), S can be determined by the lens focus and camera array size. A smaller S means a more compact sensor.

$$S = u + v,$$

$$1/u + 1/v = 1/f,$$

$$u/v = d_1/d_0,$$

where u is the optical distance from the finger to the lens, v is the optical distance from the sensor array to the lens, f is the focal length of the lens, d_1 is the finger width and d_0 is the camera array width.

The detector array of the CCD or CMOS camera is much smaller than the size of a fingerprint. Therefore, a lens serves the function of reducing magnification (focusing) by having the object distance larger than the image distance. A smaller focal length lens requires smaller optical path to image the same object and thus smaller package. However, the tradeoff for a smaller package is possible image distortion since the distance between the center of a fingerprint to the lens and the edge of the image to lens is relatively much different.

The pre-molded plastic, modular design of core optical components has been a large contributor to less expensive optical sensors. These optical parts are now uniformly precise and easy to produce in mass production. In addition, these parts are much more durable and never need calibration as did earlier optical designs. Since earlier designs were hand calibrated, there was the possibility that even the same finger has different image quality with the same type but different sensors [8,13]. Any inability to capture consistent quality images can significantly lower the reliability of recognition since fingerprint is often captured with one device and verified on another. Modular design has solved the problem.

Older optical sensors had a larger size because of the requirement that the length of the optical path from platen to lens be much longer than the size of the surface imaged. An alternative is to use multiple mirrors to maintain the optical path length, but to do so in a smaller package. The downside to this is that mirrors make the design more complicated. Usually one mirror is used in commercial scanners.

The quality of optical components also influences fingerprint image quality. Non-uniform parallel light source may cause the image brightness to be different in various image areas. Film planar light is used to create a uniform and parallel source light. As well, a prism protecting coat (such as silicone) can enhance the image, tolerate skin oils, and even protect the prism from scratching [13].

Although optical sensor has been reduced in size, it is still bulky in the context of micro-electronics. In the following section, we discuss some techniques to make the optical sensor even smaller.

3.2. Small size optical sensor

Various approaches have been developed to make smaller sized optical sensors. Sheet prism with a number of micro-prisms in the finger contact surface has been shown to reduce

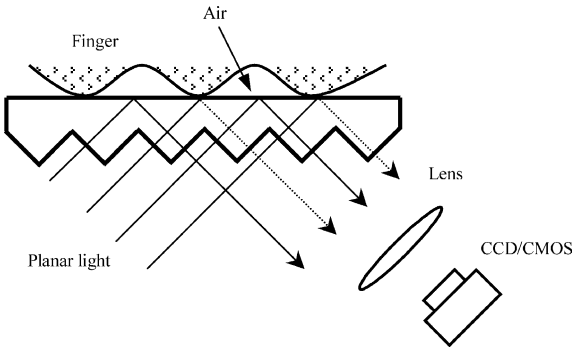

Fig. 3. Optical sensor with a sheet prism.

the size [15,16]. Fiber optics is proposed to provide optimum optical path [10,14]. A two-dimensional photo-electric image sensor is deployed to capture the image [8,10].

3.2.1. Optical sensor using a sheet prism

Traditional optical sensors have a single large prism. The sheet prism has been developed to reduce size, which has a flat surface and a number of "prismlets" adjacent to each other [16]. Each prismlet has an entrance surface and an exit surface, shown in Fig. 3. The width of the sheet is more than 10 times the maximum thickness of any one of the prismlets. Since the sheet prism is flat, the overall sensor can be very thin comparing with a traditional sensor.

This sensor also operates on the principle of FTIR. Although the prism size can be reduced, the optical path remains the same. The sensor has to use several mirrors to reduce space, at the cost of added manufacturing and adjustment complexity. A clever improvement is to include two sheet prisms stacked together [16]. It will increase the optical path in a limited space and reduce the image distortion.

The sheet prism is smaller and less expensive than a single prism. It gives the sensor an opportunity to achieve advantage with cost and size.

3.2.2. Electro-optical sensor

Optical and electronic components can be combined to create an effective sensor [8,10,17]. The design has a two-dimensional photo-electric image sensor, transparent support and light-emitting component. Because, the photo-image sensor is the same size of finger, there is no need for a lens to generate a smaller image and the optical path can be very short. This enables it to be almost as thin as a solid-state sensor.

The sensor consists of several layers, as shown in Fig. 4. The transparent layer has an outer surface upon which the finger is applied. On the inside is a two-dimensional matrix of photo-electric elements separated by strip-shaped gaps. The light-emitting layer emits the light through the strip-shaped gaps, and this passes through the transparent layer to ridges or valleys of the fingerprint. Light is reflected back at the valleys to the photo-image layer. Since the refractive index of finger and transparent layer are designed to be very close, the ridges will absorb light. The photo-electric elements are protected from light coming from the sources so as to deliver an output signal only in response to light that has been reflected towards photo-electric elements. Thus, the pattern of ridges and valleys will be generated to form a fingerprint image.

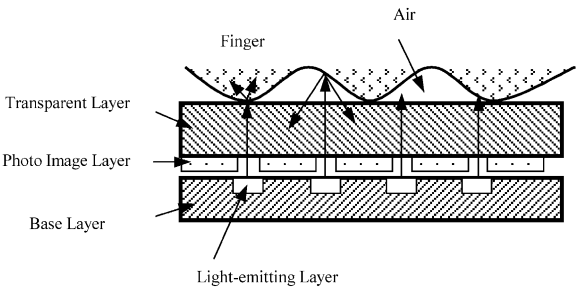

Fig. 4. Electro-optical sensor.

The photo-image layer can be made up of light-sensitive TFT (thin-film transistor) or a bundle of optical fibers [10]. The optical fiber may improve the image contrast since it has a better optical path means.

Instead of a light-emitting layer, a light-emitting polymer may be used for this type of sensor [8]. The polymer is inexpensive and can be embedded in other materials (e.g., monitor glass, laptop screen, mouse, PC card, keyboard, smart card, etc.). The size of touch area on the glass surface can be made large without the same penalty as size has for solid-state devices. Besides size, this polymer will have different characteristics (better or worse) of durability than optical or solid-state devices.

4. Solid-state sensor

Although, solid-state sensors (also called silicon or chip sensors) have been proposed in patent literature since the 1980s, it was not until the middle 1990s that these have been commercially available. Solid-state sensors were designed to address many of the shortcomings of optical sensors at the time. Optical sensors were costly, bulky, and many produced poor image quality due to dirt buildup or poor calibration. A distinct advantage of silicon sensors is the ability to integrate additional functions onto the chip. These include A/D conversion or integration of a processor core to perform all fingerprint feature extraction and matching on a single chip [18,19].

There are mainly two types of solid-state sensors: capacitive and temperature. Capacitive technology is the most prevalent [20,21]. It determines the distance to the fingerprint ridges and fingerprint valleys by measuring the electric field strength, which drops off as the inverse of distance. Temperature sensitive sensors have been designed to image

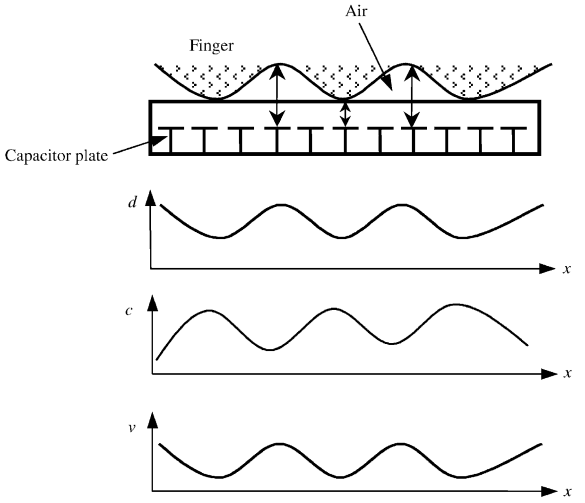

Fig. 5. Capacitive sensor.

the temperature difference of a finger related to touching ridges versus non-touching valleys [22,29].

One challenge for silicon sensors is to sustain ESD without damage. There are a number of ways manufacturers have protected their sensors: grounded enclosure, grounded metal ring around the chip, grounded metal "plugs" within the sensor array, grounded metal mesh as a top chip layer, and a very thick protective surface coating. Another challenge is cost. Since the fingerprint is large and fixed in size, chip designers cannot reduce chip size to lower cost per chip. Instead, smaller integration enables further functionality to be placed on the same size sensor to reduce system cost. We discuss another means for lowering silicon sensor cost in Section 4.2.

4.1. Capacitive sensor

There are a number of different proposed and commercial capacitive fingerprint sensors [20–24]. We describe below the general principle of how they work.

The capacitive sensor has a sensing surface on which the finger is placed. Below this surface is a two-dimension array of capacitor plates. The array is large in number, typically $300 \times 300 = 90,000$ pixels and the capacitors are small, typically 50 μm, so the entire array comprises the size of a fingerprint. The capacitors must be smaller than the width of the ridges and valleys to resolve these features. Capacitors have two plates, one plate is built within the sensor, and the other plate is considered to be the skin of the fingerprint. Capacitance varies as a function of the distance between the plates, so the fingerprint ridges and valleys can be differentiated on the basis of their capacitive measurement as illustrated in Fig. 5. The capacitive sensor also cannot be deceived by presentation of a flat photograph or printed image of a fingerprint since it measures the distances.

The capacitance C is determined by

$$C = k(s/d),$$

where C is the capacitance, k is the dielectric constant, s is the surface area of the capacitor, and d is the distance between the electrodes of capacitor. It is also known that

$$\mathrm{d}Q/\mathrm{d}t = C\mathrm{d}v/\mathrm{d}t,$$

where $\mathrm{d}Q/\mathrm{d}t$ is the change of charge over time, and $\mathrm{d}v/\mathrm{d}t$ is the voltage change over time.

As illustrated in Fig. 5, since k and s are fixed, the capacitance C changes with d. Because Q can be set by charging the capacitor to a known value, the capacitor voltage v will change when C is changed due to the distance that each ridge (closer) or valley (further) is located from the capacitor plate. Thus a fingerprint image can be determined by the measurement of the voltage output change over time at each capacitor of the sensor array.

Since fingerprint conditions vary, one of the advantages of the capacitive sensor is being able to adjust the gain to ensure the best image quality. This can be done either by adjusting the amount of charge placed on the capacitor or the amount of time that the voltage discharges [24,25]. It can be incorporated into a feedback procedure whereby the image is captured at certain settings and its quality examined by software, then the settings changed toward those to improve the quality, and this process iterated until the image quality is best. This software-controlled automatic gain adjustment enables the sensor to handle a wider range of fingerprint image quality from wet to dry and from weak to strong.

The image resolution is determined by the size of each capacitor plate. Ridges and valleys are typically 100–200 μm in width for an adult. For capacitor spacing of 50 μm (500 dpi), this yields 2–4 pixels per ridge or valley width [26]. The solid-state sensor is covered by a layer of silicon dioxide several microns thick. This layer serves as the insulating layer for ESD, physical scratching and chemical permeation protection [27,28]. A block diagram of a capacitive sensor is shown in Fig. 6. It has a sensor array of 300×300 in pixels and is fabricated from a standard CMOS process. The image capture area is 15 mm × 15 mm, and image resolution is 500 dpi. The sensor speed is 15 frames per second.

4.2. Low-cost solid-state sensor

Although the cost of solid-state sensors has brought fingerprinting accessible for personal authentication applications, products can never be too inexpensive. Solid-state sensor costs depend mainly on the area of the chip. A larger die costs more due to fewer dies per wafer and lower yield. The traditional touch sensor has a size of 15 mm × 15 mm since it has to cover the finger, which is large for a chip.

One way to obtain an image from a smaller size sensor is for the user to swipe their finger across a smaller, linear sensor, and then piece together the "line" images

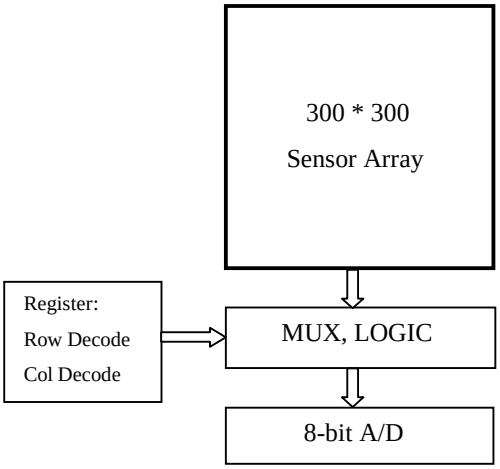

Fig. 6. Capacitive sensor block diagram.

[29–31]. The concept of swiping is widely used already. People swipe credit cards at grocery stores, key cards for entry to hotel rooms, and identity cards at company cafeterias. The size of silicon sensor can be reduced by a factor of 10 and the cost reduced commensurately. Furthermore, it is possible to capture a larger image than for touch sensors if the user swipes a longer area of the finger. The larger area will improve recognition.

In practice, a swipe sensor is not a single imaging row. Reconstruction is accomplished by determining overlap between adjacent slices by correlation, therefore, there must be some number of rows. This number relates to the speed of swiping, the speed by which the data can be accepted (via a bus or serial interface), and the reconstruction algorithm requirement on the amount of overlap. A 64-row capacitive sensor is published for the fingerprint capture [30]. The rows of the sensor can be reduced if the speed of the sensor can be increased. A thermal swipe sensor has been developed and it uses 8 rows. Since it measures temperature differences, the image is weakest when the sensor temperature is the same as the skin temperature. In Fig. 7, we illustrate a capacitive sensor that is 8 rows high, with 2–3 rows minimum of overlap.

It may be possible to construct a sensor even down to a single row if there is some means for measuring swipe speed. For instance, a mechanical roller may be rotated as the finger swipes across a single-row reader, with the rotation of the roller recording the speed [31].

The moving action across sensor may be complex and inconsistent. In some cases, a user may have to learn how to swipe to get a proper image during the first usage of swipe sensor. In an experiment we tested 35 people for swiping action. Most people can learn to become comfortable with the swiping action within 5 trials.

The slice reconstruction algorithm plays a vital role in image quality for a swipe sensor. It will rely on the overlap between adjacent slices. The slice overlaps may change because of different swiping speed and it is not a problem for reconstruction. However, there is a maximum swipe speed limit due to the sensor acquisition speed. A good reconstruction algorithm shall not sacrifice ease of use for the swipe action.

Some advantages of a swipe sensor over a touch sensor are:

- Much lower cost, $\frac{1}{5}-\frac{1}{10}$ of a touch sensor.
- Very small size, which will allow it to fit into small mobile devices such as cellular phones and PDAs.

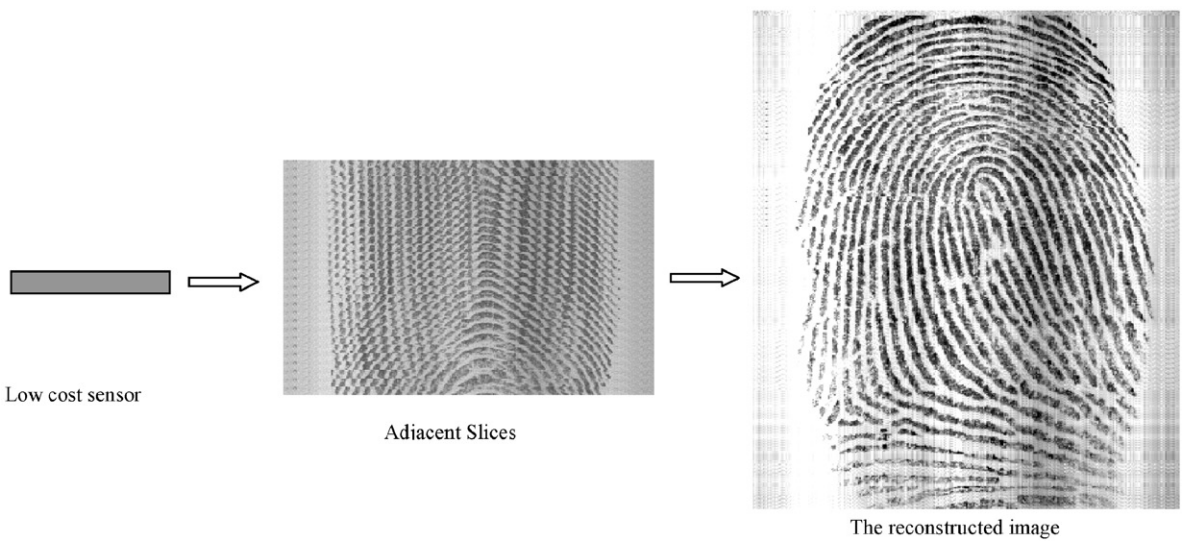

Fig. 7. Image reconstruction from a swipe sensor.

- Lower power consumption, which could be critical for handheld devices.
- Better recognition performance when a longer length image is captured.
- More durable due to smaller sensor area to damage via impact or ESD.
- Self-cleaning, the swiping action cleans the device.
- No latent image. A latent image can be left from the oil residue of a previously applied finger on a touch sensor. The swiping action leaves no more than a slice size of residue.

Since swipe sensors are just emerging it is not clear whether touch or swipe or both types of sensors will gain customer acceptance. Despite the advantages listed above, the swipe sensor does require the user to perform an action, which some users may deem an ergonomic disadvantage.

5. Summary and conclusions

Various fingerprint capture devices have been discussed in this paper. Optical sensors and solid-state sensors described along with their underlying technology, advantages and disadvantages. The recent advances in cost, size, and performance have moved fingerprint capture devices from small-volume law enforcement applications to the larger-volume arena of personal authentication. With increasing awareness of the importance of security and privacy in today's networked world, there is no doubt that fingerprint biometrics will be part of the personal authentication solution. The remaining technological advance is lower cost and smaller size. This will enable wide-ranging applications for fingerprint authentication as this solution approaches the prevalence of the metal key, but offers much higher security and convenience.

References

[1] A.K. Jain, R. Bolle, S. Pankanti, Introduction to Biometrics, Biometrics—Personal Identification in a Networked Society, Kluwer Academic Publishers, Netherlands, 1999, pp. 1–41.
[2] L. O'Gorman, Fingerprint Verification, Biometrics—Personal Identification in Networked Society, Kluwer Academic Publishers, Netherlands, 1999, pp. 42–64.
[3] J.K. Schneider, W.E. Glenn, Surface feature mapping using high resolution C-span ultrasonography, US Patent 5587533, 1996.
[4] A.K. Jain, S. Prabhakar, A. Ross, Fingerprint matching: data acquisition and performance evaluation, MSU Technical Report TR99-14, 1999.
[5] Kinetic Sciences Inc. Web pages, 2000, http://www.kinetic.bc.ca/biometrics.
[6] P.T. Higgins, Standards for the electronic submission of fingerprint cards to the FBI, J. Forensic Identification 45 (4) (1995) 409–418.
[7] J. Lan, Fingerprint imager based on a-Si:H active-matrix photo-diode arrays, ethentica and tactilesense white paper, 2000, http://www.ethentica.com.
[8] L. O'Gorman, An overview of commercial biometric systems, Workshop on Automatic Identification Advanced Technologies, Long Island, NY, 1997, pp. 23–26.
[9] M. Kawagoe, A. Tojo, Fingerprint pattern classification, Pattern Recognition 17 (3) (1984) 295–303.
[10] I. Fujieda, Y. Ono, S. Sugama, Fingerprint image input device having an image sensor with openings, US Patent 5446290, 1995.
[11] R.D. Bahuguna, T. Corboline, Prism fingerprint sensor that uses a holographic element, Appl. Opt. 35 (26) (1996) 5242–5245.
[12] STMicroelectronics image division products, 2000, http://www.vvl.co.uk/products/image_sensors.
[13] SecuGen white paper, 2000, http://www.secugen.com/index2.html http://www.secugen.com/index2.html.
[14] R.F. Dowling Jr., K.L. Knowlton, Fingerprint acquisition system with a fiber optic block, US Patent 4785171, 1988.
[15] W.S. Chen, C.L. Kuo, Apparatus for imaging fingerprint or topographic relief pattern on the surface of an object, US Patent 5448649, 1995.
[16] G. Zhou, Y. Qiao, F. Mok, Fingerprint sensing system using a sheet prism, US Patent 5796858, 1998.
[17] M. Calmel, Fingerprint sensor device, US Patent 6128399, 2000.
[18] S. Shigematsu, H. Morimura, Y. Tanabe, K. Machida, A Single-chip fingerprint sensor and identifier, IEEE J. Solid-State Circuits 34 (12) (1999) 1852–1859.
[19] S. Jung, A Low-power and high-performance CMOS fingerprint sensing and encoding architecture, IEEE J. Solid-State Circuits 34 (7) (1999) 978–984.
[20] C. Tsikos, Capacitive fingerprint sensor, US Patent 4353056, 1982.
[21] D.R. Setlak, Electric field fingerprint sensor apparatus and related methods, US Patent 5963679, 1999.
[22] D.G. Edwards, Fingerprint sensor, US Patent 4429413, 1984.
[23] A.G. Knapp, Fingerprint sensing device and recognition system having predetermined electrode activation, US Patent 5325442, 1994.
[24] A. Dickinson, R. McPherson, S. Mendis, P.C. Ross, Capacitive fingerprint sensor with adjustable fain, US Patent 6049620, 2000.
[25] M. Tartagni, R. Guerieri, A fingerprint sensor based on the feedback capacitive sensing scheme, IEEE J. Solid-State Circuits 33 (1) (1998) 133–142.
[26] D. Inglis, L. Manchanda, R. Comizzoli, A. Dickinson, E. Martin, S. Mendis, P. Silverman, G. Weber, B. Ackland, L. O'Gorman, A robust, 1.8 V, 250 μW, direct contact 500 dpi fingerprint sensor, IEEE Solid-State Circuits Conference, San Francisco, 1998.
[27] D.A. Thomas, F.R. Bryant, Electrostatic discharge protection for integrated circuit sensor passivation, US Patent 6091082, 2000.
[28] D.R. Setlak, N.W. VanVonno, M. Newton, M.M. Salatino, Fingerprint sensor including an anisotropic dielectric coating and associated methods, US Patent 6088471, 2000.
[29] J.G. Mainguet, M. Pegulu, J.B. Harris, Fingerchip: thermal imaging and finger sweeping in a silicon fingerprint sensor, Workshop on Automatic Identification Advanced Technologies, Summit, NJ, 2000, pp. 91–94.

[30] J.W. Lee, D.J. Min, J. Kim, W. Kim, A 600 dpi capacitive fingerprint sensor chip and image synthesis technique, IEEE J. Solid-State Circuits 34 (4) (1999) 469–475.

[31] Y. Fujimoto, M. Katagiri, N. Fukuda, K. Sakamoto, Fingerprint input apparatus, US Patent 5177802, January 1993.

About the Author—XIONGWU XIA received his B.S. degree in Mechanical Engineering from Zhejiang University, Hangzhou in 1994 and M.S. degree in Dept. of Precision Instrument in Tsinghua University, Beijing, China in 1997. He is a member of IEEE. Currently, he is a senior software engineer and responsible for the core fingerprint recognition engine at Veridicom Inc. His research interests include biometrics, microarray image analysis, digital image processing, pattern recognition and neural networks.

About the Author—LAWRENCE O'GORMAN is a Distinguished Member of Technical Staff at Avaya Labs Research where he works in areas of security and digital signal processing. Before this he was Chief Scientist and co-founder of Veridicom, Inc., a developer of personal fingerprint authentication systems. Prior to this he was a Distinguished Member of Technical Staff at Bell Laboratories.

Dr. O'Gorman has written over 50 technical papers, several book chapters, and two books. He has over 15 patents, and is a contributor to four biometrics and security standards. He is a Fellow of the IEEE and of the International Association for Pattern Recognition. In 1996, he won an R& D 100 Award and the Best Industrial Paper Award at the International Conference for Pattern Recognition. He is on the Editorial Boards of four journals and a member of several technical committees. He received the B.A.Sc., M.S., and Ph.D. degrees all in electrical engineering from the University of Ottawa, University of Washington, and Carnegie Mellon University, respectively.