Atmel's FingerChip™ Technology for Biometric Security

By Peter Bishop, Communications Manager

Summary

This article describes Atmel’s FingerChip technology for electronic fingerprint sensing that combines the advantages of small size, low cost, high accuracy, zero maintenance, low energy consumption and portability. This technology has applications in a wide range of fixed and portable secured devices including access control systems, cash terminals, public transport, PCs, PDAs, Smart Card readers and motor vehicles. It can be used in almost any situation where rapid, reliable and accurate identification or authentication of an individual is required.

Atmel Corporation • 2325 Orchard Parkway • San Jose, CA 95131
TEL (408) 441-0311 • FAX (408) 487-2600 • Web Site: *http://www.atmel.com*

Table of Contents

Introduction

In today's world, the need for effective security is evident. Without effective security, many everyday activities are compromised. Specific security concerns include:

- Protecting computer systems, PDAs, mobile phones, Internet appliances and similar devices from unauthorized access or use
- Protecting motor vehicles and other valuable items from unauthorized access or use
- Preventing theft and fraud in financial transactions, in particular electronic transactions, including credit card payments and payments via the Internet
- Restricting access to workplaces, warehouses and secure areas, such as military installations, to authorized personnel
- Screening access to public transportation, in particular air travel
- Authenticating the identity of an individual in drivers' licenses, health cards, ID cards, and similar administrative documents

A major factor in ensuring security is the unique identification of individuals, or the authentication that a person is who he or she claims to be. This must be done reliably, rapidly, non-intrusively and at reasonable cost. In the past, this has been done by methods such as security tokens (passports, badges, etc.), secure knowledge (passwords PIN codes, signature, etc.) or recognition by a guardian (doorkeeper). These traditional approaches are all limited with respect to the above criteria. A promising approach for the future is *biometrics*. Biometrics offers a convenient, reliable and low-cost means of identifying or authenticating individuals, and can be implemented in unsupervised and remote situations.

Biometrics seeks to identify individuals uniquely by measuring certain physical and behavioral characteristics and extracting a *sample* (also called a *sampled template* or *live template*) from these measurements in a standard data format. This sample is compared with a *template* (also called an *enrolled template* or *signature*), based on the same characteristics, that has been established as the unique identity of that individual and stored in the security system. A close match between sample and template confirms the identity of the individual.

Attention has been focused on a small number of physical characteristics that can identify individuals uniquely, notably voice, gait, face, iris and retina patterns, palm prints and fingerprints. (DNA is excluded from this list because DNA sampling is intrusive and slow.) Work is proceeding to develop electronic recognition systems based on all of these. This article focuses on fingerprints as the most advanced, mature and well-developed option.

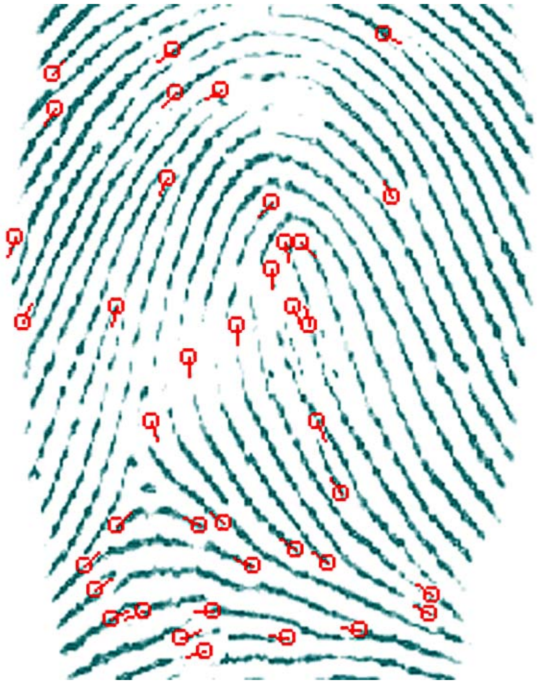
Based on centuries of experience and extensive research, fingerprints are at present considered to be the most reliable biometric for uniquely identifying an individual . In spite of some recent legal challenges in the USA, they are still regarded as giving proof of identity beyond reasonable doubt in almost all cases. The majority of the biometric-based security systems in operation today are based on fingerprint recognition.

Physiologically, a fingerprint is a configuration of *ridges* that contain individual pores, separated by *valleys*. These are supported by the underlying structure of blood vessels immediately below the skin. The morphology (shape) of a fingerprint is associated with specific electrical and thermal characteristics of the supporting skin. This means that light, heat or electrical capacitance (or a combination of these) may be used to capture fingerprint images. A fingerprint is established during fetal development, it does not change as a person ages, and it re-grows to its original pattern after an injury. After reaching adulthood, a person's fingerprints remain the same size. Identical twins do not have identical fingerprints.

A small percentage of the population (for example miners or musicians) has fingerprints that are permanently disfigured by manual activities. In developed countries, this proportion is decreasing and does not constitute a significant problem for fingerprint-based recognition systems.

There are several algorithmic methods for extracting a characteristic *template* from a fingerprint. The most popular methods are based on *pattern recognition* or *minutiae* extraction. In the case of minutiae-based algorithms, a fingerprint is characterized by gross features such as *arches*, *loops* and *whorls*, and fine features (minutiae), principally *bifurcations*, *deltas* (Y-shaped junctions) and *terminations* of ridges. Typically, between 30 and 40 minutiae are present in a fingerprint. Each of these is characterized by its position (co-ordinates), type (bifurcation, delta or termination) and orientation. See Figure 1 for an example. The set of these minutiae characteristics can provide a template for a fingerprint. Provided that these characteristics are measured sufficiently accurately, the probability of two different fingerprints having identical templates is extremely low.

Figure 1. Minutiae of a Typical Fingerprint



Electronic imaging technology and pattern recognition algorithms are now sufficiently advanced for the template of a fingerprint to be extracted automatically. In many cases standards exist for the extracted template. These standards are normally for minutia-based templates, the most notable being from the USA National Institute of Standards and Technology (NIST). However, adherence to a standard almost always limits the flexibility of the algorithm developer, and restricts the use of their proprietary intellectual property (IP). Thus there is often a tradeoff between adherence to a standard versus accuracy and speed when considering standardization.

Fingerprint Sensor Technologies

A number of different technologies for electronic fingerprint sensing are at present under development. The most widely known are optical, capacitive, radio, pressure, micro-electro-mechanical and thermal. This section outlines each of them and explains Atmel's choice of thermal as the most promising technology for its patented FingerChip product.

Optical

A variant of a digital cameras can be used to capture optical images of fingerprints. The fingertip is placed on a glass plate, suitably illuminated. A lens assembly is required that is adapted to the close proximity of the object. The image is captured by a CMOS or CCD image array with a suitable resolution, and transformed into a grayscale representation (between two and sixteen shades are generally sufficient). A disadvantage of this technique is the latent print that is left on the sensing plate that can be re-utilized. Another is the difficulty in distinguishing between live fingertips and well-molded imitations.

Capacitive

When a fingertip is placed against an array of charge-sensitive pixels, variations in the dielectric between a ridge (mainly water) and a valley (air) cause the capacitance to vary locally. This enables ridges and valleys to be identified, and an image to be constructed. Despite the vulnerability of this method to electrostatic discharge (ESD) and other parasitic electrical fields, it is one of the most popular techniques for fingerprint image capture. It is, however, relatively easy to deceive with an artificial fingertip or latent print.

Radio

If a fingertip is energized with a low-intensity radio wave, it acts as a transmitter, and the distance variation between ridges and valleys can be detected by an array of suitably tuned antenna pixels. It requires the fingertip to be in contact with the emitting region of the sensor (generally around the periphery). Because it relies on the physiological properties of the skin, it is difficult to deceive a radio sensor with an artificial fingertip. The weak point of this technique is the quality of the contact between the finger and the transmitting ring, which can also become uncomfortably hot.

Pressure

A pressure-sensitive pixel array can be constructed from piezo-electric elements that captures the pattern of ridges in a fingerprint pressed against it. Despite the numerous disadvantages of this technique (low sensitivity, inability to distinguish between real and fake fingertips, susceptibility to damage from excessive pressure, etc.) some companies are pursuing this approach with product prototypes.

Micro-electro-mechanical

Micro-electro-mechanical systems (MEMS) are on the cusp between R & D and deployment in a number of applications. An array of micro-mechanical sensors that detects the ridges and valleys in a fingertip has been constructed in laboratories, but the robustness of such a device is not assured. It would also be impossible to distinguish between a real and an artificial fingertip by this method.

Thermal

Pyro-electric material is able to convert a difference in temperature into a specific voltage. This effect is quite large, and is used in infrared cameras. A thermal fingerprint sensor based on this material measures the temperature differential between the sensor pixels that are in contact with the ridges and those under the valleys, that are not in contact.

The thermal approach has numerous benefits. These include strong immunity to electrostatic discharge, and the absence of a signal transmitted to the fingertip. Thermal imaging functions as well in extreme temperature conditions as at room temperature. It is almost impossible to deceive with artificial fingertips.

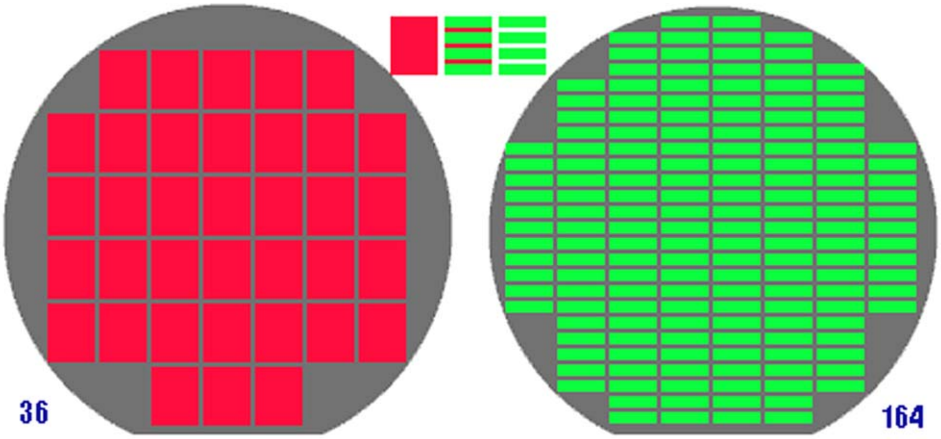
A disadvantage of the thermal technique is that the image disappears quickly. When a finger is placed on the sensor, initially there is a big difference in temperature, and therefore a signal, but after a short period (less than a tenth of a second), the image vanishes because the finger and the pixel array have reached thermal equilibrium. This is one of the reasons for using a scanning technique for image capture, described below.

Static or Scanned Image

Most of the above technologies for image capturing can be applied in two different ways. One is to use a static image capture window that is the same size as the required fingerprint image and hold the fingertip against the window for the time interval required to capture the image. This approach has the advantage of capturing an entire image in one operation. Its significant disadvantages include the large die size required (and therefore increased IC cost, see Figure 2), and the fact that a latent print is retained on the image capture window.

The second approach is to use a rectangular window that is the width of the required image and only a few pixels high, and sweep the fingertip vertically over it. This approach requires the image to be scanned in sections and re-constructed by software. Its advantages include a significantly reduced die size (and therefore IC cost), a stable image in the case of thermal capture and the fact that it is self-cleaning. No latent print remains on the image window after a scan. This method is mandatory for thermal image capture due to the short duration of the temperature differential.

Figure 2. Reduced Die Size Decreases IC Unit Cost



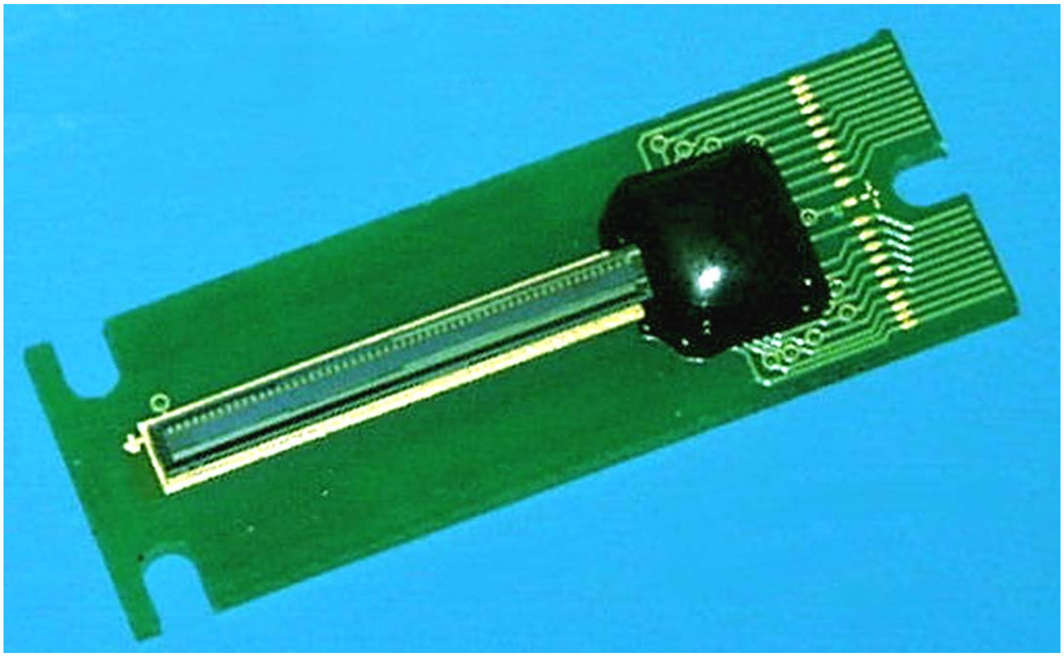
Atmel's Choice: Scanned Thermal Imaging

The combination of thermal image capture and a scanning window gives the benefits of small die size, low unit cost, passive operation, reliable functionality over a wide range of environmental conditions and security against artificial fingertips or the re-use of latent images. These benefits have led Atmel to its choice of scanned thermal imaging for its FingerChip IC.

FingerChip Technology

Atmel's AT77C101B FingerChip IC for fingerprint image capture combines detection and data conversion circuitry in a single rectangular CMOS die. It captures the image of a fingerprint as the finger is swept vertically over the sensor window. It requires no external heat, light or radio source. See Figure 3.

Figure 3. The FingerChip Die Mounted on a Chip-on-Board (COB) Support



The FingerChip Sensor

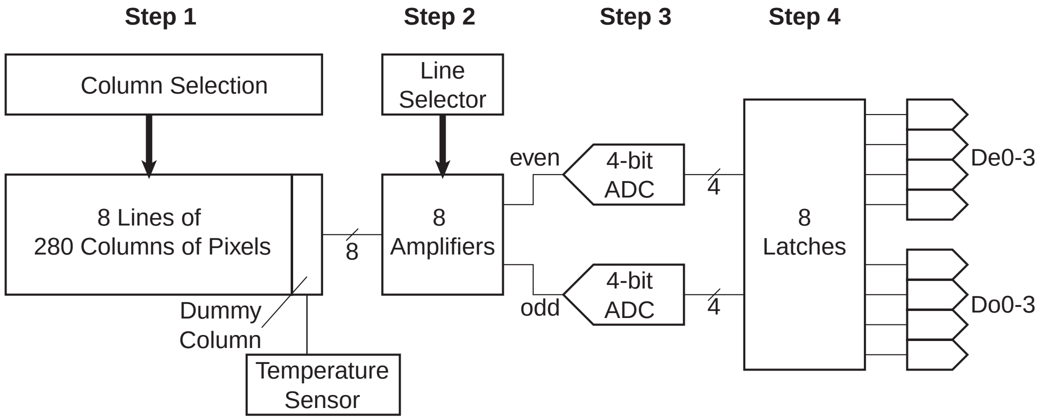
The FingerChip sensor comprises an array of 8 rows by 280 columns, giving 2240 temperature-sensitive pixels. An additional dummy column is used for calibration and frame identification. The pixel pitch of 50 µm by 50 µm provides a resolution of 500 dpi over an image zone of 0.4 mm by 14 mm. This is adequate to capture a frame of the central portion of a fingerprint at an acceptable image resolution. This resolution also complies with the Image Quality Specification (IQS) from the IAFIS (Integrated Automated Fingerprint Identification System) of the U.S. Federal Bureau of Investigation (FBI).

The pixel clock is programmable at up to 2 MHz, giving an output of 1780 frames per second. This is more than adequate for a typical sweeping velocity. An image of the entire fingerprint is re-constructed from successive frames using software provided by Atmel.

FingerChip Functionality

The FingerChip sensor and data conversion circuitry are fabricated on a single monolithic die measuring 1.7 mm by 17.3 mm. The functional elements are shown in Figure 4.

Figure 4. FingerChip Functional Diagram



The cycle of operations for each frame is as follows:

1. One column is selected amongst the 280 + 1 in the sensor array. Columns are selected sequentially from left to right with wraparound. After reset, output commences from the leftmost column.
2. Each pixel in the column sends its temperature value as an analog signal to the bank of amplifiers.
3. Two lines at a time are selected (odd and even) to send their amplified analog values to the 4-bit analog-to-digital converters (ADCs). These analog values are also available as outputs (not shown in the functional diagram).
4. The two four-bit digital equivalents are latched and sent in parallel as one byte via the parallel outputs De0-3 (even line) and Do0-3 (odd line).

Figure 5 shows the sequence of outputs for one frame, and Figure 6 shows the succession of frames that are output continuously while the FingerChip is in active mode.

Figure 5. FingerChip Frame Output

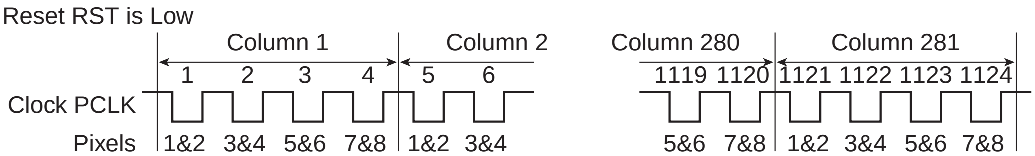
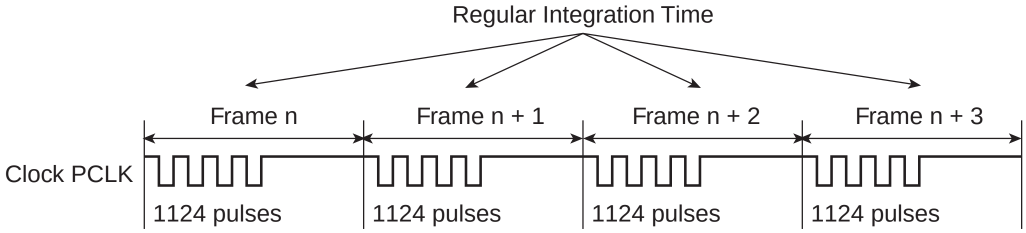


Figure 6. FingerChip Frame Sequence



FingerChip Features

FingerChip possesses a number of outstanding features that make it ideally suited for a variety of demanding security applications.

In terms of robustness, the IC is naturally protected against electro-static discharges (ESD) up to at least 16 kV. The frame window is resistant to abrasion, being qualified for up to at least one million finger sweeps. It is also able to resist considerable applied pressure.

FingerChip's operating voltage is 3.3V to 5V, with a power consumption of 20 mW at 3.3V, 1 MHz. This is equivalent to approximately 7 mA on the power supply pin. It features a nap mode with reset enabled, clock stopped, temperature stabilization disabled and output disabled to put the output lines in high-impedance state. In nap mode, power consumption is limited to leakage current only.

In normal operation, the sensor is entirely passive, using the thermal energy in the applied fingertip to obtain its measurements. However, if the temperature differential between the finger and the sensor falls too low (less than one degree) a temperature stabilization feature is activated to slightly raise the temperature of the IC and recover the contrast.

FingerChip Benefits

The benefits of the FingerChip technology derive from its thermal sensing technique, its frame sweeping method of image capture, and the integration of the sensor and data conversion circuitry as a single IC.

The thermal sensing approach requires no signal transmission to the fingertip, making use of the physiological properties of a live fingertip. This reduces its power requirements, and any potential discomfort to the person associated with energizing the fingertip with current or radio waves.

The sweeping method of image capture reduces the silicon area required by the sensor array by a factor of 5, leading to a similar reduction in unit cost. The re-constructed image is, however, of a high resolution. It also means that the sensor window is self-cleaning, with no latent prints left after an image capture. If a person is being forced to provide a fingerprint impression, an erratic movement of the fingertip over the window (or a fingertip saturated in sweat) will prevent an image from being obtained. Independent tests have also established that it is difficult to sweep an artificial fingertip smoothly enough to enable an image to be re-constructed.

Integrating the image sensor and conversion circuitry in a single CMOS IC reduces costs and power consumption, and increases operational speed. It also makes it possible to integrate encryption or other application-specific circuitry on the same die or in a stacked die package for enhanced security.

Fingerprint Recognition Systems

Fingerprint recognition can be used in a wide range of applications, but they all require the same set of basic procedures. These are independent of the technology used for fingerprint sensing, and the software used for template and sample extraction and comparison.

Enrolment and Matching

As an initial step, the fingerprints of the identified population are *enrolled*. Operationally, fingerprints are captured and compared against the database of enrolled individuals, or a subset of it (in the limit, one single enrolled fingerprint). This process is known as *matching*.

Enrolment consists in capturing and storing the reference version of the fingerprint of an identified individual. Needless to say, this must take place under secure circumstances, without the possibility of an imposter giving the fingerprint, or of the data obtained being tampered in any way. The fingerprint obtained, or the set of data extracted from it, is known as the *template* (also called *enrolled template*) of the individual.

During the operation of the system, for example at the point of entry to a secure building, fingerprints are captured and processed in the same ways as during enrollment. The data obtained, known as a *sample* (also called *sampled template*), is compared against the set (or a subset) of templates. If a *match* is obtained, the individual presenting the sample is *identified*. (If the sample is compared against a single template, for example to confirm the identify the owner of a Smart Card, the process is known as *authentication* or *validation*.)

Both enrolment and matching follow the same initial series of data processing steps, as explained below in the context of FingerChip.

Image Acquisition

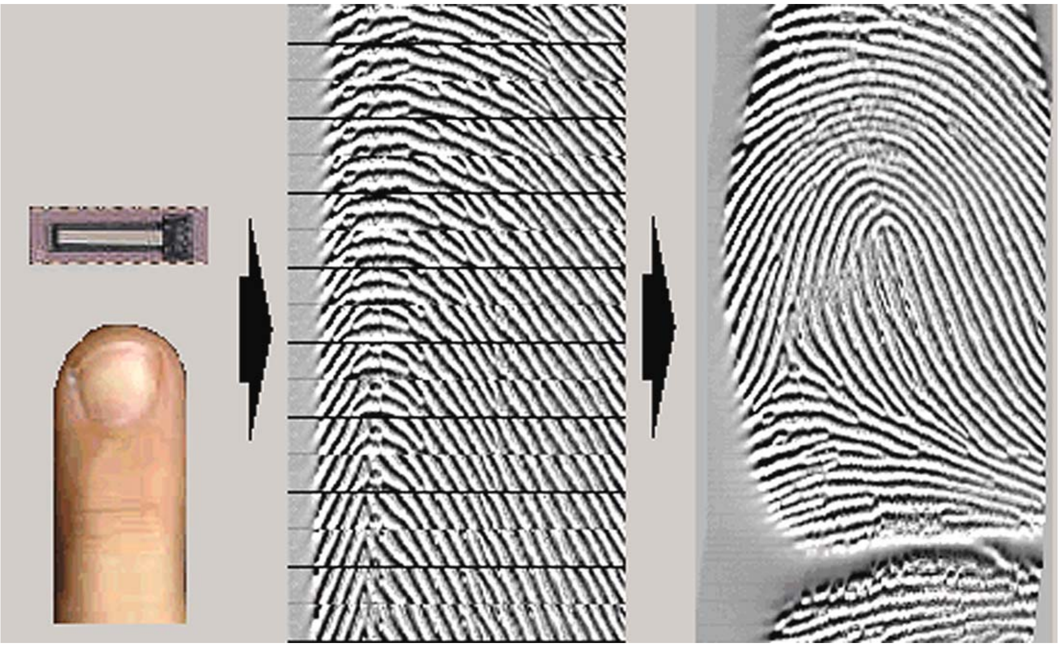
Image acquisition consists in obtaining a bitmap, at an adequate resolution, of all or part of the fingerprint. The way that this is done by FingerChip is explained in the previous section. The outcome of this step is a sequence of horizontal frames, each 8 x 280 pixels at 4-bit resolution, that together give the complete image of the fingerprint.

Image Reconstruction

Provided that the fingertip has been swept across the sensor window at a reasonable rate, the overlap between successive frames enables an image of the entire fingerprint to be reconstructed. See Figure 7. This is done using software supplied by Atmel as part of the FingerChip deliverable. The reconstructed image is at 8-bit resolution due to resolution enhancement during frame reconstruction. This in compliance with the FBI IQS specification mentioned previously.

The reconstructed image is typically 25 mm x 14 mm, equivalent to 500 x 280 pixels. At 8-bit resolution per pixel, this requires 140K bytes of storage per image. Larger or smaller images can be derived from this, using standard image processing techniques, depending on the requirements of the application.

Figure 7. Fingerprint Image Reconstruction



Template or Sample Extraction

For reasons of security, and due to data storage limitations, it is not advisable to store images of entire fingerprints in the fingerprint recognition system. (A reference image may be stored in a secure location during enrolment as a backup and for access in exceptional circumstances; but it is not required for the normal functioning of the system.) The normal procedure is to extract a unique *template* from the image, using pattern recognition or the principle of minutiae as described before. During enrolment, this gives the enrolled template, and during verification it gives the sampled template. The procedure is identical in both cases.

There are several reasons for this:

- A typical set of 36 minutiae, each requiring four bytes of storage, occupies only 144 bytes. This is a considerable compression from the file size of the entire image.
- The fingerprint cannot be re-constructed from the template. This reduces the possibility of fraudulent use of the data by electronic intruders or dishonest employees.
- The template can further be compressed by any standard data compression algorithm, and it can also be encrypted if required. This is important for applications such as fingerprint-enhanced Smart Cards, where data storage space is at a premium, and high security is essential.

Template extraction is performed by third-party software, generally following an industry-standard procedure for the identification and description of minutiae, and their representation.

Template/Sample Matching

The final stage in the matching procedure is to compare the sampled template with a set of enrolled templates (identification), or a single enrolled template (authentication) if the identity of a single person is being established.

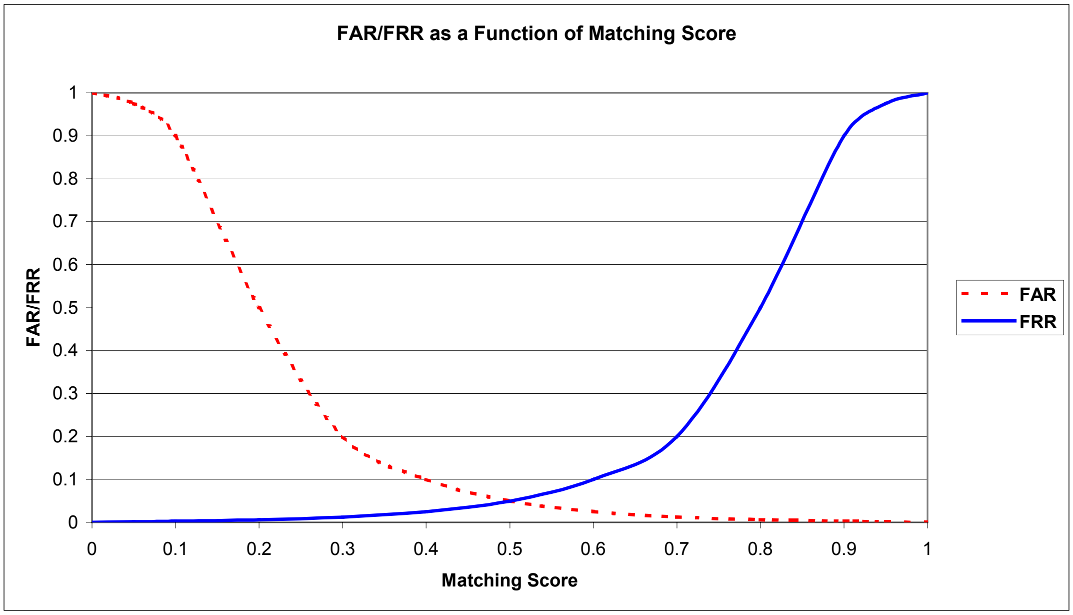
It is highly improbable that the sample is bit-wise identical to the template. This is due to approximations in the scanning procedure (at 50 µm resolution this is far from exact), mis-alignment of the images and errors or approximations introduced in the process of extracting the minutiae. Accordingly, a *matching algorithm* is required that tests various orientations of the image and the degree of correspondence of the minutiae, and assigns a numerical *score* to the match. Above a certain (arbitrary) level, a match is declared.

This gives rise to two possible types of error:

- **False Acceptance**, where a non-corresponding sample and template give a high enough score to be accepted. This permits an imposter to be accepted by the system. The probability of this occurring is the False Acceptance Rate (**FAR**).
- **False Rejection**, where a corresponding sample and template do not produce a high enough score to create a match. This results in an enrolled person being rejected by the system. The probability of this occurring is the False Rejection Rate (**FRR**).

The **crossover rate** is the point where the FAR and FRR rates intersect as a function of the matching score. See Figure 8 (hypothetical FAR/FRR values).

Figure 8. FAR/FRR as a Function of Matching Score[1]



Note: 1. The crossover rate is the point where the curves intersect.

All fingerprint recognition systems attempt to minimize both FAR and FRR, but in practice there is a tradeoff between the two. Reducing the FAR increases the FRR and vice-versa. The cutoff point for acceptance/rejection needs to be adjusted in order to minimize the consequences of the two classes of error. In most cases false acceptance is more serious, because an imposter is admitted by the system, with all the consequences that entails. The consequences of false rejection can range from annoying to life threatening, depending on the application, in particular whether there is an alternative or manual backup system available.

Some systems are sophisticated enough to include an intermediate area between acceptance and rejection, where additional information or action is requested by the person seeking identification. For example, the person may be requested to re-scan the same finger, or scan another finger if a second template is available.

The process of template/sample matching is carried out entirely by software, and is independent of the technology used for fingerprint capture. However, a high-quality image is essential to keep the FAR and FFR to a minimum.

Atmel's Strategic: Positioning in the Security Market

Strategic Security Focus

Atmel has a strategic commitment to the market for electronic security systems. A range of complementary integrated circuits is being developed to serve this market, often in collaboration with market leaders in end-user security products. The result is ICs that are closely adapted to the requirements of their particular market segment. These are supported by software drivers and third-party applications modules that provide security system developers with a solution that combines performance (from hardware) and flexibility (from software).

Markets for Security Products

The market for secure identity products is extremely diverse. At present it is partitioned into the following broad segments:

- **Login** access to PCs, PDAs, Internet Appliances and similar devices
- **Electronic key** access to motor vehicles and other high-value objects
- **Financial transactions**, including Smart Cards and their readers, ATMs (cash terminals) and Internet transactions
- **Access control**, including entry to buildings, stadiums, public open spaces and secure installations such as military installations, or secure areas in any of these
- **Transportation**, including road, tunnel and bridge tolls and screened access to subway, bus and air travel
- **Administrative applications**, including health, social security, passports, drivers' licenses and ID cards.

All of these are high-growth markets where electronic products are a long way from saturation. For example, Smart Cards are well established in parts of Europe but are just starting to be introduced in the USA, and are likely to leapfrog older technologies such as magnetic stripe cards in Asia. The potential market runs to billions of units.

These markets demand mixture of products with electrical contacts (such as Smart Cards and their readers), contactless products (such as radio road toll transponders) and sensors (such as fingerprint readers).

Summary of Atmel's Security Products

Atmel is developing complementary ICs that address all segments of the security products market, as described above. These ICs fall into five broad categories:

- **Sensors**, including FingerChip, CCD and CMOS image sensors.
- **Radio Frequency (RF) ICs**, including RFID tags and RF front-end elements for other secure applications. Many of these are based on Silicon-Germanium (SiGe) technology.
- **Secure Memories**, including secure EEPROMs with sectors that are locked/unlocked by a challenge/response system.
- **Secure Microcontrollers**, including the secure AVR® Flash-based 8-bit RISC microcontroller for Smart Cards and other secured applications.
- **Secure ASSPs**, including a PC security module that implements the Trusted Computing Platform Alliance (TCPA) specification for Trusted Platform Modules (TPM).

These elements can be used together in an end-user application. A typical combination is a sensor or RF front-end for data capture, a secure microcontroller for processing and one or more secure memories for storage. These ASSPs and standard products can also be used as system-on-chip building blocks for highly-integrated customer-specific ICs (ASICs) in high-volume applications.

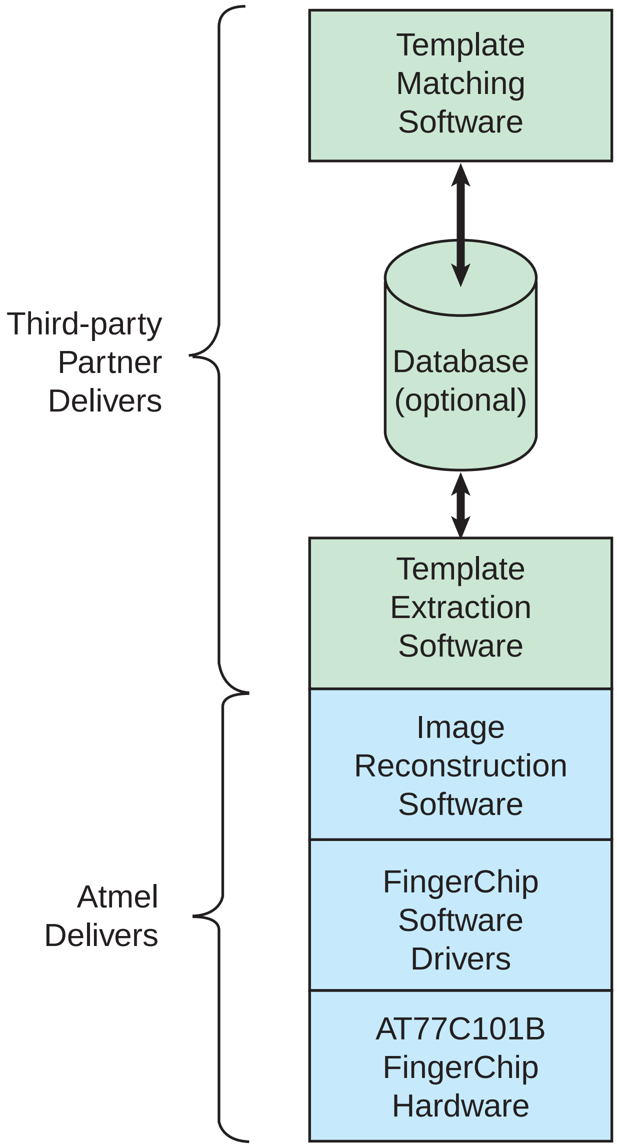
FingerChip Deliverables, Business Model and Roadmap

Atmel's business model for FingerChip is to develop and market the AT77C101B FingerChip IC together with software drivers for common operating systems and image reconstruction software. These are supported on common hardware platforms including ARM®, StrongARM®, Intel® XScale™ and Texas Instruments® DSPs. Operating Systems include Windows® CE and Linux®.

Application-specific software such as that for minutiae extraction and sample/template comparison is being developed by qualified third-party suppliers with whom Atmel works in partnership on a non-exclusive basis. This strategy enables customers to benefit from the performance, reliability and low cost of Atmel ICs while retaining the choice of the most appropriate software provider for the specific requirements of the end-user product.

Atmel's deliverables and modules provided by third-parties are shown in Figure 9.

Figure 9. FingerChip Deliverables


Template Matching Software
Database (optional)
Template Extraction Software
Image Reconstruction Software
FingerChip Software Drivers
AT77C101B FingerChip Hardware
Third-party Partner Delivers
Atmel Delivers

The roadmap for the FingerChip product builds on the basic thermal image capture technology with a succession of higher-performance interfaces including USB and SPI. This leverages the core product into a successively broader field of applications.

Application Examples

Application Scenario: Smart Card and Reader with Fingerprint Authentication

For reasons of confidentiality, the example given below is hypothetical. It shows how Atmel's FingerChip IC can be combined with other Atmel products in a representative security application.

In order to provide a higher level of security than that given by a conventional PIN code, a Smart Card can be loaded with an encrypted template of the fingerprint of its owner. When using the Smart Card, the owner provides (in addition to the PIN code) a fingerprint sample to the Smart Card reader as a further means of authentication. Atmel can supply all of the ICs used in such a system, in both the Smart Card and the reader, as ASSPs or standard products. They are illustrated in the system block diagram in Figure 10.

Figure 10. Smart Card Reader with Fingerprint Authentication

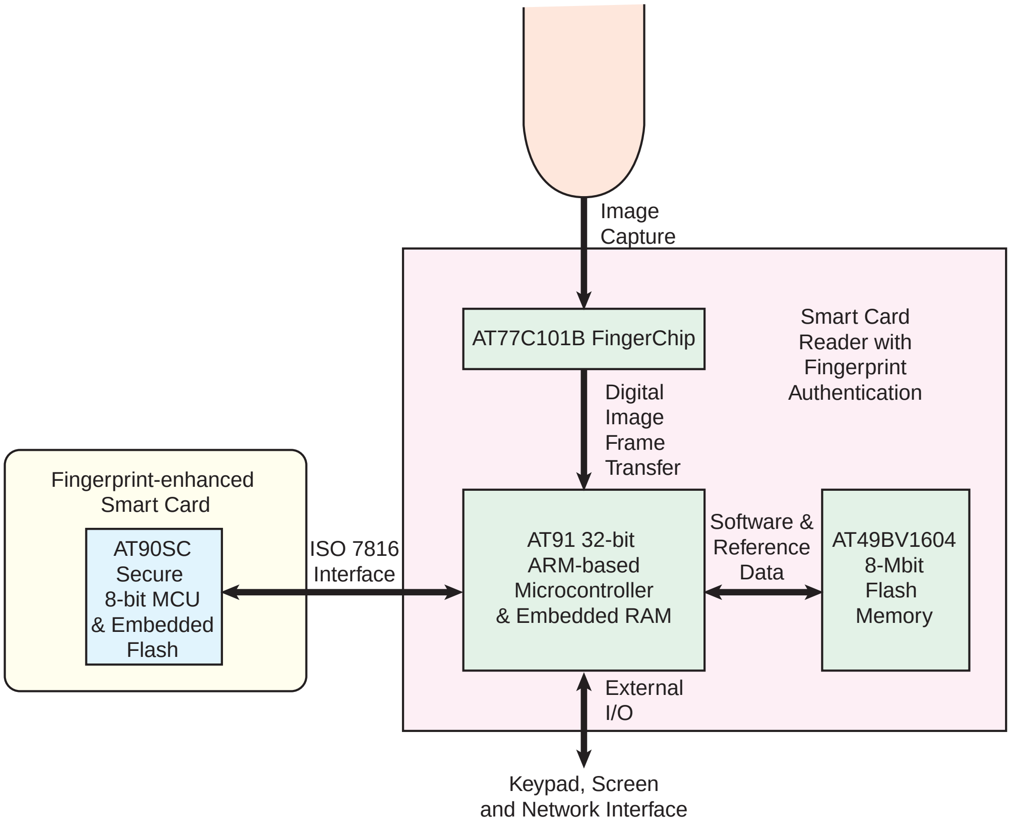


Image Capture
AT77C101B FingerChip
Smart Card Reader with Fingerprint Authentication
Digital Image Frame Transfer
Fingerprint-enhanced Smart Card
AT90SC Secure 8-bit MCU & Embedded Flash
ISO 7816 Interface
AT91 32-bit ARM-based Microcontroller & Embedded RAM
Software & Reference Data
AT49BV1604 8-Mbit Flash Memory
External I/O
Keypad, Screen and Network Interface

The fingerprint-enhanced Smart Card contains an AT90SC secure 8-bit microcontroller with embedded Flash memory. This memory contains (in addition to the software and reference data) an encrypted version of the fingerprint template that is loaded during the enrolment of the Smart Card owner. The Smart Card reader is built around an AT91 32-bit ARM-based microcontroller with an AT49BV Flash memory for program and reference data storage. Communication between the AT90SC and AT91 is via an industry-standard ISO 7816 secure interface. Fingerprint image capture and digitization is carried out by the AT77C101B FingerChip.

At the start of the authentication operation, the AT90SC in the Smart Card is activated by the AT91 in the reader and a conventional PIN code entry/validation is carried out. This is done via the ISO 7816 interface. This provides an initial level of confidence in the validity of the Smart Card and the person claiming to be its owner.

The fingerprint of the person claiming to be the Smart Card owner is then captured by the FingerChip, digitized and sent to the AT91microcontroller. The AT91 re-constructs the image from the sequence of frames and extracts the sample from it. It then encrypts the sample and uploads it to the AT90SC in the Smart Card. The AT90SC compares the encrypted sample that it has received from the fingerprint reader with the encrypted template stored in its secure memory. If the matching score is sufficiently high, it sends a confirmation message to the AT91 in the reader. The person is authenticated as the owner of the Smart Card, and the associated transaction is authorized.

This procedure is known as *match-on-card*. It ensures that the encrypted fingerprint template never leaves the Smart Card, and that the sample is sent to the Smart Card only in encrypted form.

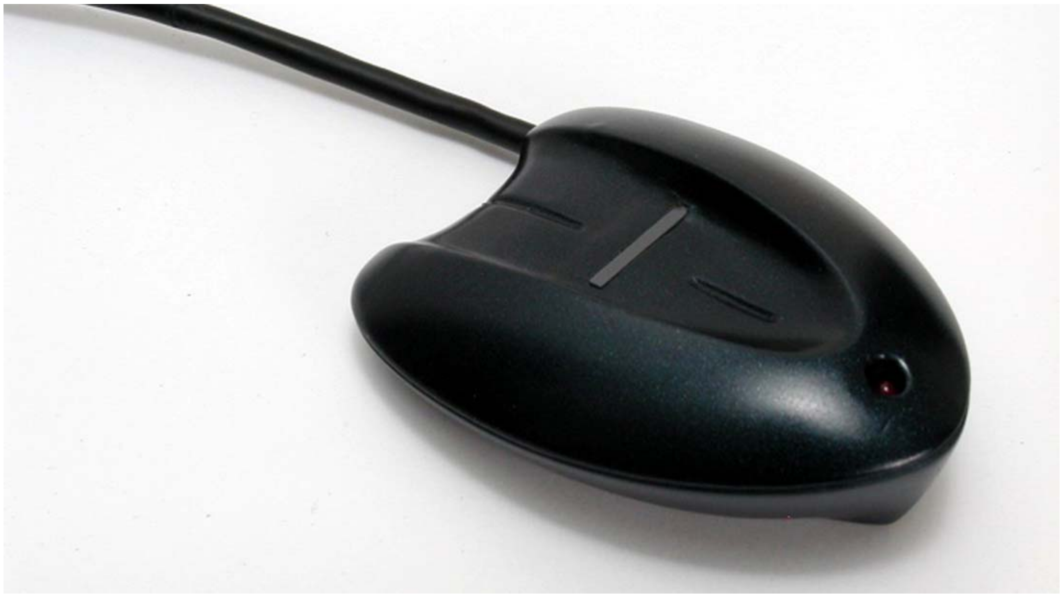
The numerous benefits of this system include the low component count, which keeps size, power consumption and cost to a minimum. The AT91 and AT49BV ICs can be encapsulated in a single package for further size and cost reduction. The use of ASSPs and standard products eliminates the NRE (Non-Recurring Engineering) costs of custom IC development. Flash memory in both the Smart Card and the reader allows for system upgrades based entirely on software. The acceptance/rejection cutoff point can be adjusted by software according to the security requirements of the application, and it is a matter of an additional software module to require one or more additional fingerprint scans in doubtful cases.

No fingerprint templates or samples are permanently stored on the reader – the encrypted template never leaves the Smart Card, and the sample is erased after each authentication operation. This eliminates the need for access to a database of enrolled templates and greatly reduces the possibilities for fraudulent use of this data.

Bioki Fingerprint Reader and Biothentic Fingerprint-enhanced Smart Card Reader

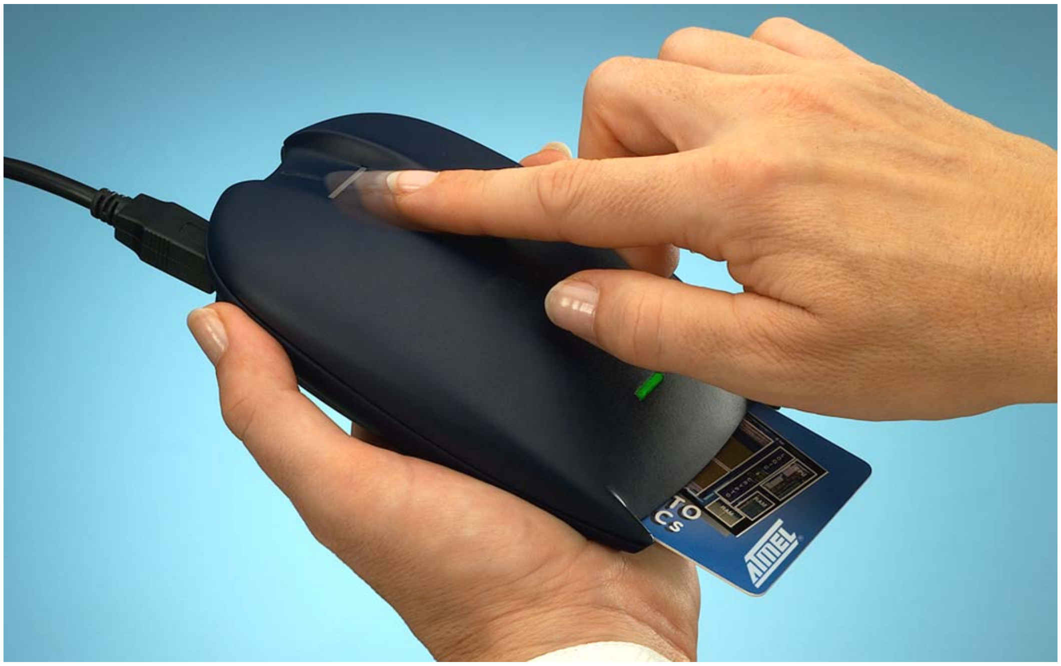
The Bioki Fingerprint Reader (Figure 11) from ID3 provides secure access to PCs. It functions as a PC peripheral, connected via a USB bus. Using a FingerChip IC and biometrics software from ID3, it captures the image of a fingerprint, and can enroll and authenticate authorized user(s) of the PC system.

Figure 11. ID3 Bioki Fingerprint Reader



Also from ID3, the Biothentic Smart Card reader with fingerprint sensor (Figure 12) implements the match-on-card application scenario described in the previous section. It includes a FingerChip and two ISO 7816-compliant Smart Card interfaces. It is aimed at a wide range of secured electronic transactions, including electronic commerce and ID card authentication.

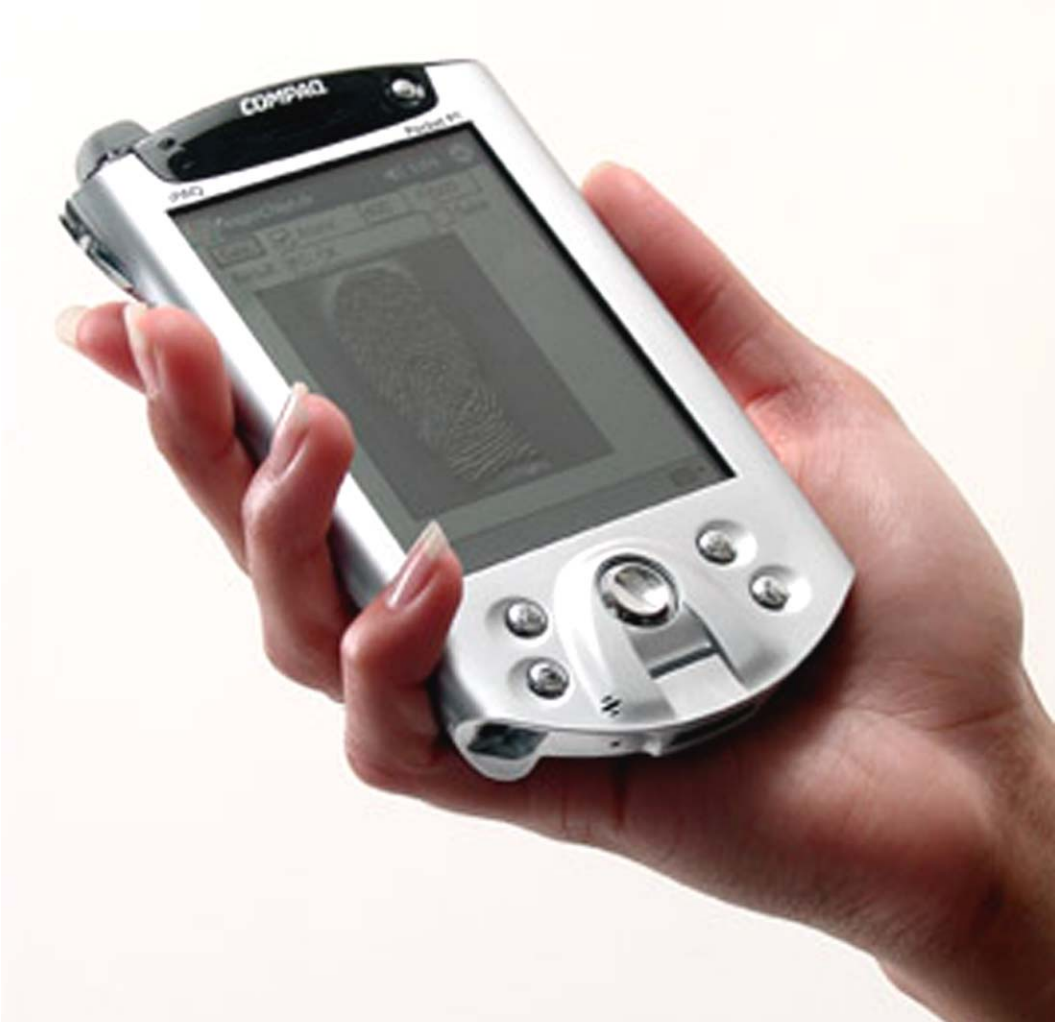
Figure 12. ID3 Biothentic Smart Card Reader with Fingerprint Sensor



iPAQ h5400 Pocket PC

The iPAQ® h5400 Pocket PC from HP® (Figure 13) is a multimedia PDA that integrates Atmel's FingerChip for biometric login authentication. It relieves the user of the task of memorizing and updating login passwords, and makes it almost impossible for a lost or stolen device to be used by someone else.

Figure 13. HP iPAQ h5400 Pocket PC with FingerChip for Biometric Login



Amongst the additional features of the h5400 is wireless LAN access using the AT76C503A IEEE 802.11b/USB Wireless LAN Media Access Controller (MAC), also from Atmel.

Conclusion

Atmel has selected fingerprint recognition as the most established means of biometric identification, and thermal imaging as the means of image capture that offers the highest possible reliability at minimal cost. This is the basis of its FingerChip product. A complete security system can be constructed using Atmel ASSPs and standard products together with industry-standard software that combines performance and flexibility with low development and production costs. Atmel's Flash memory technology allows for system upgrades with no substitutions of its ICs.

Biometrics is an emerging activity that is likely to become an integral part of our daily lives, creating an enormous on-going market for products based on state-of-the-art technology such as the Atmel FingerChip.

References

1. Common Biometric Exchange File Format (CBEFF), January 2001, USA National Institute of Standards and Technology (NIST), Web http://www.nist.gov

2. FBI Integrated Automated Fingerprint Identification System (IAFIS), USA Federal Bureau of Investigation, Web: http://www.fbi.gov/hq/cjisd/iafis

3. Smart Cards and Biometrics in Privacy-Sensitive Secure Personal Identification Systems, May 2002, Smart Card Alliance, Web: http://www.smartcardalliance.org/

4. The Biometric Consortium, Web: http://www.biometrics.org

5. International Biometric Industry Association (IBIA), Web: http://www.ibia.org

6. BioAPI Consortium, Web: http://www.bioapi.org

7. London Metropolitan Police, Web: http://www.met.police.uk

8. Ridges and Furrows (Private Web Site),
Web: http://www.ridgesandfurrows.homestead.com

Editor's Notes

About Atmel Corporation

Founded in 1984, Atmel Corporation is headquartered in San Jose, California with manufacturing facilities in North America and Europe. Atmel designs, manufactures and markets worldwide, advanced logic, mixed-signal, nonvolatile memory and RF semiconductors. Atmel is also a leading provider of system-level integration semiconductor solutions using CMOS, BiCMOS, SiGe, and high-voltage BCDMOS process technologies.

Further information can be obtained from Atmel's Web site at www.atmel.com.

Contact: Peter Bishop, Communications Manager, Atmel Rousset, France, Tel: (+33) (0) 4 42 53 61 50, e-mail: pbishop@atmel.com