Access Control Using Fingerprint Authentication Processor and RFID

HATIM A. ABOALSAMH
Computer Science Department
King Saud University
P.O. Box 51178 , Riyadh 11543
Kingdom of Saudi Arabia
Hatim@ksu.edu.sa http://faculty.ksu.edu.sa/aboalsamh

Abstract: A typical access control system uses two components. First component is a fingerprint reader that is connected to a database to match the pre stored fingerprints with the one obtained by the reader. The second component is an RFID card that transmits information about the person that requests an access. In this paper, a compact system that consists of a CMOS fingerprint sensor (FPC1011F1) is used with the FPC2020 power efficient fingerprint processor ; which acts as a biometric sub-system with a direct interface to the sensor as well as to an external flash memory for storing finger print templates. The small size and low power consumption enables this integrated device to fit in smaller portable and battery powered devices utilizing high performance identification speed. An RFID circuit is integrated with the sensor and fingerprint processor to create an electronic identification card (e-ID card). The e-ID card will pre-store the fingerprint of the authorized user. The RFID circuit is enabled to transmit data and allow access to the user, when the card is used and the fingerprint authentication is successful.

Key-Words: Access control, RFID, Fingerprint processor, Fingerprint authentication, Biometrics.

1 Introduction

Biometrics technology is based on identification of individuals by a physical or behavioural characteristic. Examples of recognition of physical characteristics are: fingerprints, iris, face or even hand geometry. Behavioural characteristic can be the voice, signature or other keystroke dynamics. What make fingerprints idealistic for personal digital identification is the fact that the fingerprint pattern is composed of ridges and valleys that form a unique combination of distinguishing features of each finger (as shown in Figure 1); also, fingerprint characteristics do not vary in time [1].

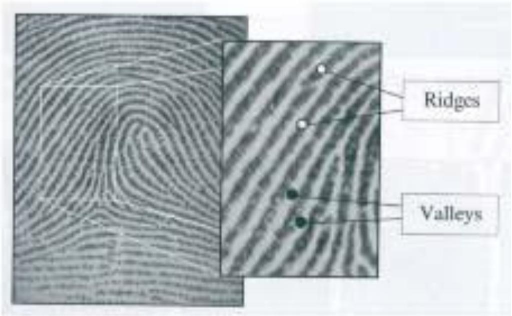


Figure 1: An illustration of Ridges and Valleys in finger prints

New technologies introduced compact CMOS fingerprint sensor, such as the FPC1011F1 with several significant advantages:

a) Delivers superior image quality, with 256 gray scale values in every single pixel.
b) Ergonomically; the sensor component is suitable for numerous types of authentication systems.
c) Could be highly integrated with low power solutions utilizing Fingerprint microprocessor such as FPC2020 chip, or a large variety of standard microcontrollers.

A compact CMOS fingerprint sensor is used with the FPC2020 fingerprint processor ; which acts as a biometric sub-system with a direct interface to the sensor and an external flash memory for storing templates. The small size and low power consumption of this system enables it to be embedded in a Variety of devices , such as, card readers, and smaller portable devices without losing performance.

If The sensor and fingerprint processor could be integrated with an RFID circuit to create an e-ID card. The e-ID card will pre-store the fingerprint of the authorized user. When the card is used and the authentication is successful; the RFID circuit is enabled to transmit data and allow access to the user.

Some of the useful Application for such a device would be : Computer peripheral, Physical access control, Time and attendance, Wireless devices, Security application, and Medical equipment & storage.

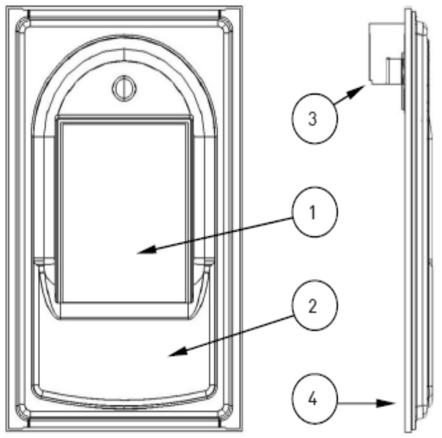
The idea of this e-ID card is to have a portable authentication functionality as well as access control through the RFID circuit; all in one package in a credit card size.

2 System components

The system is divided into three main components: the fingerprint sensor, the fingerprint processor, and the RFID circuit.

2.1 The fingerprint sensor

The FPC1011F1 (see Figure 2) is a new compact CMOS fingerprint sensor with several significant advantages. The FPC1011F1 delivers superior image quality, with 256 gray scale values in every single pixel. The reflective measurement method sends an electrical signal via the frame directly into the finger. This technique enables the use of an unbeatably hard and thick protective surface coating. The sensor with its 3D pixel sensing technology can read virtually any finger; dry or wet. Thanks to the new hard and durable surface coating, FPC1011F1 is protected against ESD well above 15 kV, as well as scratches, impact and everyday wear-and-tear. FPC1011F1 is delivered with a designed micro ergonomic guidance frame, simplifying proper fingerprint guidance and hence improving algorithm performance.



ITEM DESCRIPTION

1	FPC1011 fingerprint area sensor chip
2	Drive electrode, called frame or bezel
3	Flex film connector: 8 pin, 1 mm pitch Molex / 0528520870 / low insertion force
4	BT substrate

Figure 2: The FPC1011F1 compact CMOS fingerprint sensor.

2.1.1 The FPC1011F1 fingerprint sensor reference data

1. Dimension Sensor body (W x L x T), nominal 20.4 x 33.4 x 2.3 mm
2. Interface Serial SPI 8 pin
3. Supply voltage VDC, typical 2.5 - 3.3 V
4. Supply current Typical at 3.3V, 4MHz and RT (room temp) 7 mA
5. Supply current sleep mode Power down, typical 10 µA
6. Clock frequency Serial SPI 32 MHz
7. Read out speed Serial SPI 4 Mpixel/s
8. Active sensing area Pixel matrix 10.64 x 14.00 Mm
9. Size sensing array Pixel matrix (363 dpi) 152 x 200 Pixel
10. Pixel resolution 256 gray scale values 8 Bit
11. ESD protection IEC61000-4-2, level 4, air discharge > 15 kV
12. Wear-and-tear No of wear cycles at 6N > 1 million Cycle

2.1.2 Architecture of the FPC1011F1 fingerprint sensor Package

As shown in Figure 3 , the sensor package consists of several vital components to read the fingerprint and transform the reading into a greyscale representation of the fingerprint. The readout is then stored in a serial flash memory as a template.

The sensor area is a matrix of 152x200 elements that represent pixels. Once the finger is positioned over the sensor, a voltage is supplied through the TX1 line. The voltage is moved through the finger to the elements of the sensor matrix. Each matrix will hold a voltage value. Those values are deferent, since they represent ridges and valleys of the fingerprint. The sensor element values are transferred in sequence through the X and Y address registers. Each sensor element is converted through an A/D circuit to a digital value that represents a gray scale pixel (values between 0 and 255). The pixels are then transferred to a serial flash memory and organized into a template. The memory template represents a gray scale image of the fingerprint[2].

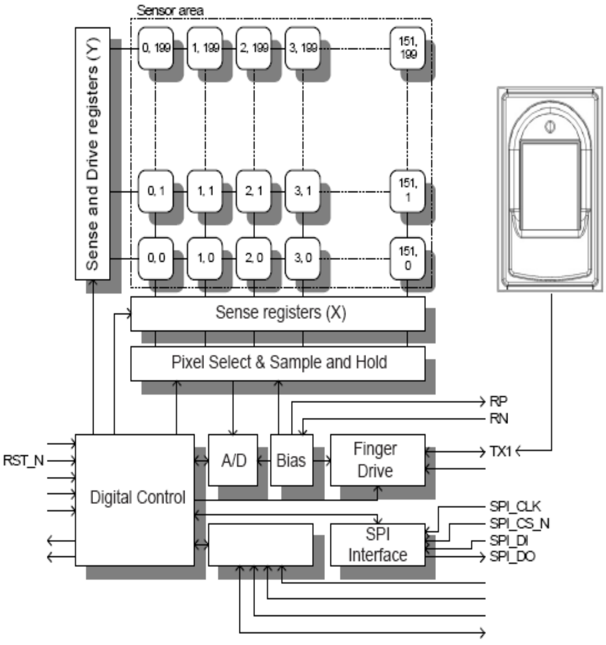


Figure 3: Architecture of the FPC1011F1 fingerprint sensor [2].

2.2 The Fingerprint Processor

The FPC2020 is a small, fast and power efficient ASIC that acts as a biometric sub-system with a direct interface to the FPC1011C sensor as well as to an external flash memory for storing templates. Thanks to its small size and low power consumption it fits as well in door locks, card readers and safes as in smaller portable and battery powered devices without losing identification speed or performance. FPC2020 can easily be integrated into virtually any application and be controlled by a host sending basic commands for enrolment and verification via the serial interface. Fingerprint templates are created automatically and stored in flash memory connected to FPC2020. Templates used for verification can also be uploaded/downloaded to an external storage, e.g. central database, smart card or portable flash memory. FPC2020 has no internal limitation in number of templates it can handle. Size of external flash memory will set the limitation [3]. The pin out configuration of FPC2020 processor is shown in Figure 4.

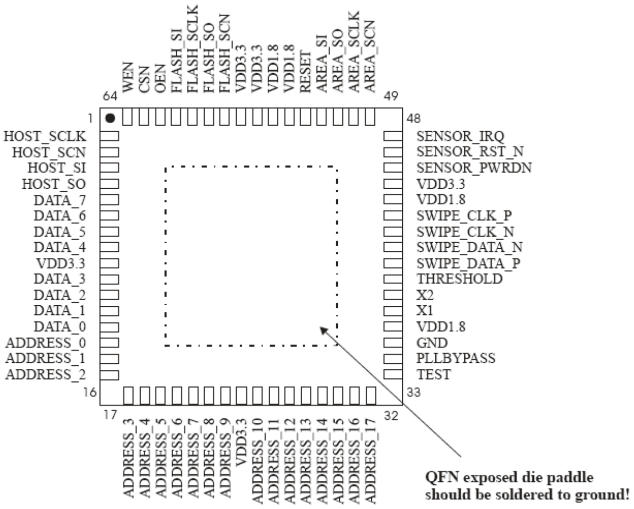


Figure 4: The 64 pin out configuration of FPC2020 processor [3].

2.2.1 The Finger Print Processors instruction set

The FPC2020 processor has over 80 instructions. The instruction set is divided into (7) groups [3].:

1. Biometrics commands
2. Image transfer commands
3. Template Handling Commands
4. Algorithm setting Commands
5. Firmware Commands
6. Communication Commands
7. Other supplementary commands

The instructions from the first groups is listed, and their description are shown in tables (1) as an example [3].

BIOMETRIC COMMANDS	HEX	DESCRIPTION
API_CAPTURE_IMAGE	0x80	Capture image from sensor (before enrol).
API_CAPTURE_AND_ENROL_RAM	0x81	Enrol into RAM (includes Capture Image)
API_CAPTURE_AND_VERIFY_RAM	0x82	Verify against RAM (includes Capture Image)
API_CAPTURE_AND_VERIFY_FLASH	0x83	Verify against single FLASH slot (includes Capture Image) Set slot number in IDX
API_CAPTURE_AND_IDENTIFY_FLASH	0x84	Identify against all FLASH slots (includes Capture Image)
API_ENROL_RAM	0x85	Enrol into RAM
API_VERIFY_RAM	0x86	Verify against RAM
API_VERIFY_FLASH	0x87	Verify against single FLASH slot Set slot number in IDX
API_IDENTIFY_FLASH	0x88	Identify against all FLASH slots
API_CAPTURE_IMAGE_ FINGERPRESENT	0x89	Capture Image from sensor (once a finger is present)
API_ENROL_FLASH	0x92	Enrol into FLASH memory
API_CAPTURE_AND_ENROL_FLASH	0x93	Enrol into FLASH memory (includes Capture Image)

Table 1: Biometrics commands

3 The Application Program

The application program is stored into the auxiliary memory connected to the fingerprint processor. The program start executing once the finger is positioned over the sensor package. The program consists of instructions to read the sensor area and match it with a pre stored fingerprint template. If the pre stored template matches the image in the sensor area then the processor sends a signal to enable the RFID circuit.

4 The RFID circuit

RFID tags come in a variety of different types according to their functionality, and these types have been defined in an RFID Class Structure by the Auto-ID Centre (and later through EPC Global), which has been subsequently refined and built on. The basic structure defines five classes in ascending order as follows [4,5]:

Class	*Class Layer Name*	*Functionality*
1	Identity Tags	Purely passive, identification tags
2	Higher Functionality Tags	Purely passive, identification + some additional functionality (e.g. read/write memory)
3	Semi-Passive Tags	Addition of on-board battery power
4	Active *'ad hoc'* Tags	Communication with other active tags
5	Reader Tags	Able to provide power for and communicate with other tags i.e. can act as a reader, transmitting and receiving radio waves

Table 2: RFID Class Structure by the Auto-ID Centre

5 RFID circuit used in this system

The microID® 125 kHz MCRF200 is a passive Radiofrequency Identification (RFID) device for low-frequency

applications (100 kHz-400 kHz). The device is powered by rectifying an incoming RF signal from the reader. This device has a total of 128 bits of user programmable memory and an additional 12 bits in its configuration register. The user can manually program the 128 bits of user memory by using a contactless programmer in a
microID developer kit such as DV103001 or PG103001 [6].

6 System Integration

The reader is a handheld or fixed unit that can interrogate nearby RFID tags and obtain their ID numbers using radio frequency (RF) communication (i.e. the process does not require contact). When a passive tag is within range of a reader, the tag’s antenna absorbs the energy being emitted from the reader, directs the energy to ‘fire up’ the integrated circuit on the tag, which then uses the energy to beam back the ID number and any other associated information as shown in Figure 5.

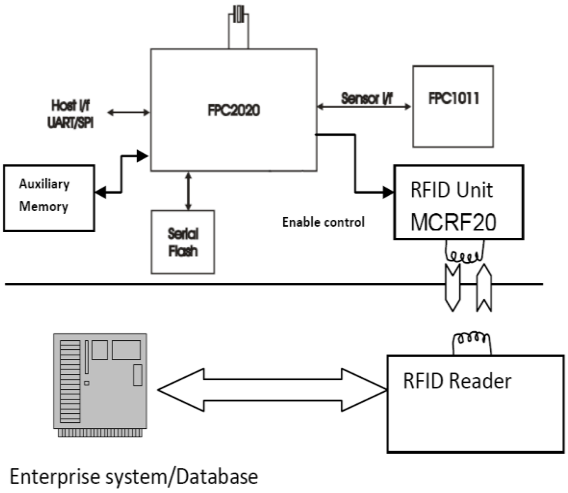


Figure 5: System Integration

7 Conclusion

The e-ID consists of a compact CMOS fingerprint sensor (FPC1011F1 fingerprint sensor Package) connected to the FPC2020 fingerprint processor; which acts as a biometric sub-system with a direct interface to the sensor as well as to an external flash memory for storing templates. The small size and low power consumption enables this integrated device to fit in card readers and in smaller portable and battery powered devices without losing identification speed or performance. The sensor and fingerprint processor is integrated with an RFID circuit to create an e-ID card. The e-ID card will pre-store the fingerprint of the authorized user. When the card is used and the authentication is successful; the RFID circuit is enabled to transmit data to the RFID reader which reads the information transmitted and allow access to the user. The e-ID design enables the authentication without the need for a huge database of fingerprints of authorised users and external fingerprint reader. Hence the proposed system will save time since it has one matching operation to perform, and will save cost since no external fingerprint readers are needed.

References:

[1] Salah M. Rahal, Hatim A. Aboalsamh, Khalid N. Muteb, Multimodal Biometric Authentication System- MBAS, *2nd IEEE International Conf. On Communication & Technologies: From Theory to Applications*, , April 24-28, 2006, Vol. 1, 24-28, pp. 1026-1030.

[2] The FPC1011F1 Area sensor Package product specifications, www.fingerprints.com

[3] The FPC2020 fingerprint processor , www.fingerprints.com

[4] RFID: Frequency, standards, adoption and innovation, *JISC Technology and Standards Watch*, May 2006.

[5] Klaus Finkenzeller, *RFID-Handbook, 2nd edition*, Wiley & Sons LTD., 2003.

[6] System Design Guide microID® 125 kHz RFID, *Microchip Technology Inc.* , 2004.