IEEE ISIE 2005, June 20-23, 2005, Dubrovnik, Croatia

Hardware-Software Co-design of an Automatic Fingerprint Acquisition System

Fons M*, Fons F*, Canyellas N*, Cantó E*, López M**

* Escuela Técnica Superior de Ingeniería ETSE-URV, Tarragona, Spain

** Escuela Universitaria Politécnica de Vilanova i la Geltrú EUPVG-UPC, Barcelona, Spain

Abstract—**Nature has provided human beings unique and different each one in relation to the others; even 'identical' twins have infinite differences between them. Every individual has his own biological characteristics that allow him to be distinguished from the rest of the humanity.**

In recent years, biometrics and computer technology have joined together in order to improve the security in everyday activities such as access control systems, cash terminals, public transport, internet, smart card readers… where user identification/authentication is required before giving him access to confidential information, relevant places or restricted resources. In any situation where rapid, accurate, reliable and secure identification or authentication of an individual is required, electronics and biometrics take place. With biometrics-based security systems there is no longer any need to remember a large number of PINs and passwords, so the genuine biometric characteristics of every individual play the role of personal identity code in front of the world.

The first stage in these identification systems is the biometric characteristic acquisition. The authors focus their work on that field in the specific case of using fingerprints as biometric feature. A good solution is detailed from a 'performance vs cost' point-of-view.

I. Introduction

The different tasks involved in any biometric recognition process are always the same, independently of the biometric feature selected to build the system (iris, retina, ADN, hand geometry, voice, fingerprints…). In the first stage, called *enrolment*, the user enrols himself in the recognition system. To do this, the system measures one particular biometric (physical or behavioural) characteristic of the user. From the measurement it generates a *template* or identity code associated to the user, and stores it together with the user's name (ID) and other personal data in a protected data base or a smart card. After the *enrolment* phase, the user becomes available in the system so he can be properly recognized or identified in the second stage of the recognition process: the *authentication* phase. During *authentication*, the user's biometric characteristic is measured again. A new *template* is generated from the current measurement and compared with the previously-stored *template*. If both are similar enough, it is assumed that the user whose *template* was stored at *enrolment* phase is present. Otherwise, it is assumed that the user who tries to be authenticated is an impostor.

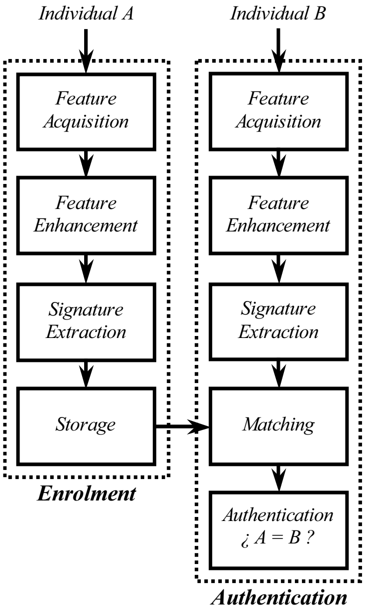

Figure 1. Biometrics-based personal authentication system.

Most of the biometrics-based security systems in operation today are based on fingerprint recognition and electronic embedded technologies [1], [2], [3]. The current silicon-based fingerprint sensors have the performance of small size, low cost, high accuracy, zero maintenance and low consumption. These advantages make them suitable for automated recognition systems. Moreover, embedded systems such as those based on *System-on-Chip* devices can be compared to small computers: they can store a personal key in such a way that it can never be read from outside and only used internally by the system itself so, the data are well protected against external attacks. The new generation of *trusted smart cards* is a good example about that: they integrate the biometric sensor in the own smart card becoming then secure portable devices, able to perform all the steps related to the recognition process.

II. Fingerprint Recognition Systems

The well-known characteristics of uniqueness and permanence related to human fingerprints are the basis of any user's fingerprint recognition system [3], [4]. Fingerprints are in fact the oldest biometric signs of identity. The first fingerprint recognition systems were performed for law enforcement purposes, and the

0-7803-8738-4/05/$20.00 ©2005 IEEE

fingerprint acquisition was done manually by means of ink and paper. Nowadays however, the application range of fingerprint biometrics has taken off: computers, cellular phones, smart cards, PDAs, cars… until the point that wherever you use a key, a PIN or a password, it can be replaced by your own fingerprint. Electronic fingerprint sensors and capture methods have been developed in order to automate the acquisition process and enhance the performance of prior solutions.

The trend on personal recognition is the design of compact electronic systems able to perform all the stages involved in the identification/authentication process [5]. The first stage in any automated fingerprint recognition system is the fingerprint acquisition. It consists of obtaining a digital image of the fingerprint. Typically, fingerprint acquisition systems use *ridges* and *valleys* for recognition, and a sensor resolution of 500 dpi (dots per inch) –which corresponds to a sensing surface of 50 x 50 microns square per pixel– is good enough to get relevant signal information. In some other cases however, fingerprint *pores* may be also used. In that case, and due to the fact that *pores* are roughly 40 microns wide, higher resolution (about 1000 dpi) is required for the sensor in the acquisition stage.

The resolution of the acquired image is normally 4 or 8 bits per pixel, that is 16 or 256 grey-scale image respectively. In some applications however, there are also systems that use only 1 bit per pixel or binary fingerprint images. It will depend obviously on the next stages linked to the process, such as *signature extraction*, *storage* and *matching* algorithms implemented in the recognition system, or even the memory space requirements of the application.

Image acquisition is a critical step, not only for *enrolment* stage, but also for *authentication* phase. Subsequent recognition stages will only be effective if the acquired bitmap is a good quality image, so special attention must be taken during acquisition. If not, the system fails.

Bad hardware interface (sensor + microcontroller) or bad acquisition processing software will give bad results; and even both, good hardware and good software, may give bad results if they are not well suited to each other.

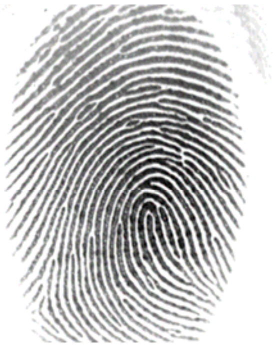

Figure 2. Fingerprint ridges and valleys (500 dpi resolution).

Apart from the efficiency of the acquisition system, there is also the quality of human fingerprints that has to be taken into account. Close to 90% of the population have ‘good’ quality fingerprints: wet and flexible skin with well-defined ridges and valleys. The other 10% of the population however have ‘bad’ quality fingerprints: dry and poor or worn ridges, due to factors such as their job (miners, farmers…) or age. But a recognition system needs to work properly for everybody so, this becomes another significant concern related to the intrinsic reliability of fingerprint-based identification systems.

III. Fingerprint Based Sensors

The aim of fingerprint acquisition systems is to capture fingerprints in an automatic way so electronic sensors are required.

There are several fingerprint sensing techniques:

♦ Optical sensors. It is difficult to integrate them in embedded electronic systems due to its high cost and large volume. This is basically because of their prisms, lens, camera, as well as their required focal lengths and mechanical assembly.

♦ Ultra-sound sensors. They have the advantage of reading the *derma* or sub-surface of the skin rather than the surface, solving then the concern about poor quality fingerprints. Moreover, it is possible to know if the sensed finger is alive or dead, adding thus more security to the system. Ultra-sound sensing however, requires a large device with mechanical parts and tends to be quite expensive. As optical sensors, this option is not suitable for embedded systems at low cost.

♦ RF sensors. These sensors inject a low radio frequency signal into the finger and each pixel then acts like an antenna. It is possible to detect if there is a ridge or a valley in the finger according to the local conductivity of the skin and the local electrical field read by every sensing pixel. This technique is nowadays available but hardly used.

♦ Silicon-based sensors. There are two factors that allow silicon-based sensing to be the most useful technique to be integrated in embedded biometric recognition applications:

- its easy integration with CMOS technology,
- and its low cost.

Several techniques have been proposed to perform fingerprint sensing:

• Pressure: based on the idea that when you apply your finger on a surface, the ridges of your finger automatically apply a pressure over the sensor, whereas the valleys do not apply such a pressure. Unfortunately, the resulting sensitivity is very low and such devices do not have a good performance.

• Capacitance: this is one of the most popular techniques, based on the measurement of the capacitance between the skin (ridge-valley) and the sensing pixel. As the distance between the sensing pixel and the ridge or the valley varies, so does the capacitance. One of the most important weak points of such devices is the vulnerability to electro-static discharges that could damage the device. Another non secure characteristic is due to the fact that it is frequent to keep latent fingerprint images on the sensing surface after the acquisition stage.

- Thermal: it is becoming one of the most secure techniques due to the fact that the image vanishes after a short period of time as the finger and the surface sensor reach thermal equilibrium, avoiding latent images on the sensing surface after the acquisition. It is based on pyro-electric material and temperature physical effects, enabling the conversion of temperature differentials into voltages. The pyro-electric material that is in direct contact with the skin's ridges measures the temperature of the skin, whereas the pyro-electric material under the valleys equals the ambient air temperature.

In silicon-based chips, it is easy to state that lower area means lower cost. In order to reduce their cost the sweeping technique has been developed. The user sweeps his finger over a rectangular shaped sensing array of several pixels tall. To enable image reconstruction without taking into account the finger sliding speed, the acquisition frequency has to be high enough to guarantee the overlap of several rows between consecutive acquired slices. An image processing task is then required to reconstruct the fingerprint image from the acquired slices.

The fingerprint sweeping technique is nowadays widely used in capacitive and thermal sensors, achieving good results in terms of accuracy, reliability and cost.

The authors focus their work on a commercial thermal sweeping sensor that presents a sensing area of 0,4 mm x 14 mm. The image array consists of 8 x 280 pixels, allowing the acquisition of the fingerprint image by sweeping the finger across the sensing area. The device captures a programmable number of images per second, while two integrated 4-bit analog-to-digital converters transform and deliver them simultaneously into a 8-bit digital signal adapted to electronic interfaces such as microprocessors and microcontrollers.

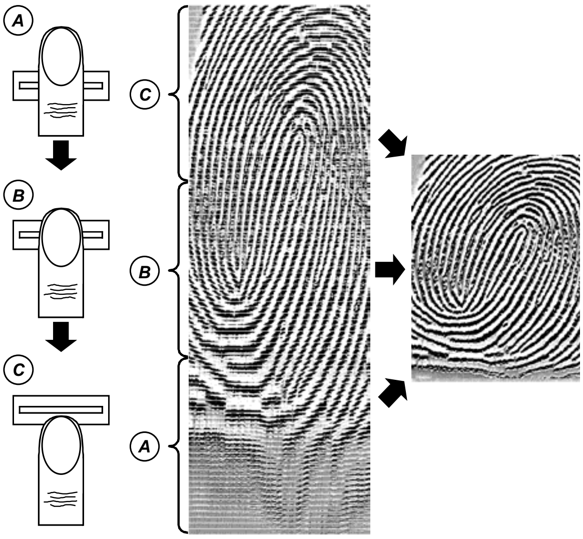

Figure 3. Fingerprint sweeping technique.

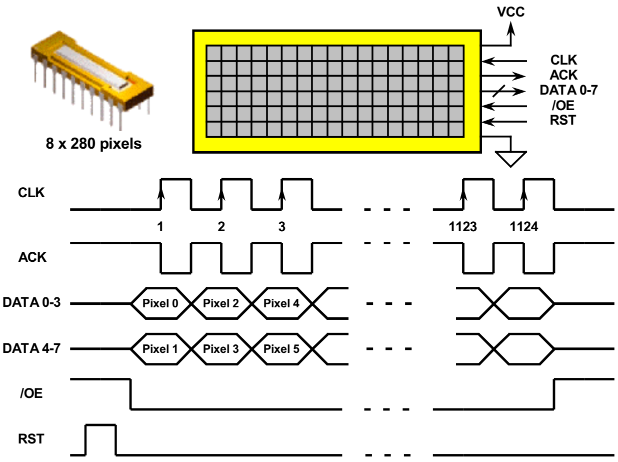

Figure 4. Thermal sweeping sensor features.

Each pixel is a sensor in itself. The information of every pixel is coded with 4 bits, so a total of 2 pixels are coded in one byte. As it is shown in figure 4, the status of 2 pixels is transmitted from the sensor to the external controller (DSP, ASIC, µP, µC, FPGA …) at a time, every rising edge of the system clock. The external controller acts as a master, taking control of the acquisition process, whereas the sensor device acts as a slave.

IV. System-on-Chip Based Architecture

It is important to remark that absolute security does not exist. However, there are a lot of ways to increase the security of any system at a reasonable or even low cost.

Sweeping technique can improve the security of any acquisition system, removing the chance of latent whole fingerprint images on the sensor after the acquisition process, and reducing at the same time the total cost of the sensor and the total size of the system.

Moreover, the overall organization of the system can improve its security level. The system-on-chip technology is a good example about that: integrating all or some electronic components (such as the microcontroller, its memory block, a programmable logic device such as a FPGA, and some logic peripherals) of a whole system in a single device is an appropriate solution from a performance point-of-view: reliability, security and cost issues [6]. Regarding to reliability, less devices means less system complexity and also more system reliability. Regarding to security, the fact that the main components of a system are on a chip reduces the presence of external buses so all the internal buses, the internally stored data and the processing performed inside the device are well protected against external attacks. And finally, system-on-chip technology and its associated EDA tools allow Hw-Sw co-design and co-verification of high-performance systems at low cost, improving the time-to-market of the final product.

The authors focus their work on a platform based mainly on a SoC device integrating a microcontroller, its memory block and a dynamically reconfigurable FPGA; as well as a fingerprint sweeping sensor device, as it is shown in figure 5. The main purpose of this architecture is in fact to improve the reliability and the security of the final application, reducing at the same time the overall system cost by means of reducing the amount of system silicon area and lowering also the total power consumption. It is possible to partition any application in hardware and software tasks, thus synthesizing in the FPGA such higher computationally intensive tasks while the microprocessor will be executing the rest of less complex tasks and controlling also the FPGA reconfiguration. The microprocessor can either reconfigure the entire contents of the FPGA or individual elements of the FPGA while others elements are currently active, without decreasing the throughput of the overall application.

V. Hardware-Software System Co-design

The authors drive their work to the following end: the implementation of an automatic system able to verify the identity of a person by means of the biometric features of his own fingerprints. In fact, nowadays such a biometric system there already exists, but implemented usually by software under complex computer platforms performing very expensive computational tasks [7]. Therefore, one of the final goals is to justify that it is possible to implement a biometric identification system without so much amount of resources and getting similar results in accuracy and speed terms. The main purpose of this work is to define the electronic architecture that permits to reach high performance at low cost. Is for this reason that authors use the system-on-chip technology, the sweeping technique, and define a low cost platform with hardware-software co-design performance and dynamically reconfigurable hardware. This article is focused on the first stage of any biometric verification process: the feature acquisition. In the following points it is detailed how an *Automatic Fingerprint Acquisition System* is designed.

A. Overview

The system architecture in based on a platform with 2 main components: the commercial FPSLIC® SoC device and the FINGERCHIP® sweeping sensor, both from Atmel Corporation® [8], as it is shown in figure 5.

The FPSLIC *(Field Programmable System Level Integrated Circuit)* incorporates one 8-bit microprocessor, its memory block (36 kbytes of program + data memory), some fixed peripherals such as 3 programmable timers, 2 serial UARTs, one I2C controller, an 8-bit hardware multiplier module as well as 2 I/O programmable ports, and a programmable logic device that incorporates up to 40000 gates and dynamic reconfigurability performance in only one chip.

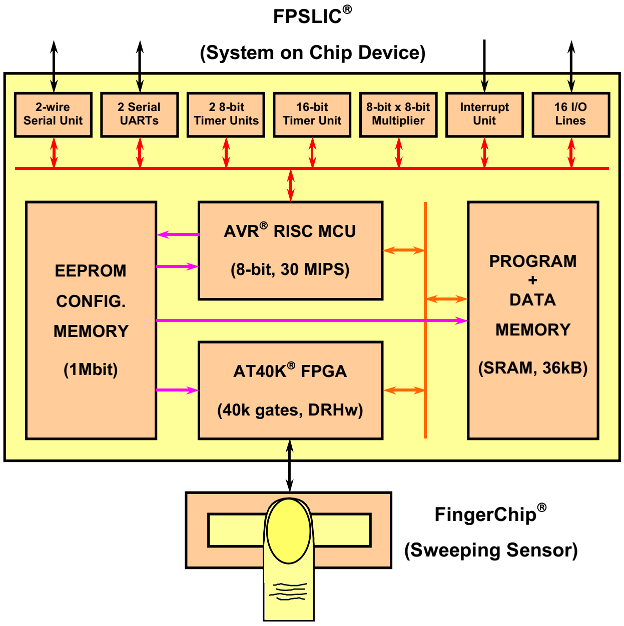

Figure 5. System architecture.

The FingerChip sweeping sensor is managed from the SoC. The whole sensing area of the sensor (a frame composed by 8 lines of 280 pixels) is sensed sequentially at the clock frequency given by the SoC device. Therefore, the SoC drives the clock to the sensor, and simultaneously, the SoC reads up to 2 pixels (2 x 4 bit data) at a time. After 1124 clocks, a complete slice is read.

In order to allow the correct acquisition of the different slices and the following reconstruction process of the fingerprint image, it is necessary to get the consecutive slices at a frequency high enough to insure overlap between frames, independently of the finger sliding speed through the sensing surface. It has been checked that a minimum slice acquisition rate of 200 frames per second is good enough to acquire and reconstruct good quality images with a fair sliding speed for the finger. While acquiring consecutive slices, the fingerprint image has to be reconstructed 'on-the-fly' by combining the slices as they are captured by the sensor, and delivered to the SoC. The acquisition and reconstruction process is shown in figure 6.

To speed up the system, the image reconstruction process has to be performed concurrently with the image acquisition process, so just after acquiring the last slice of the finger, the whole fingerprint image has to be ready and properly stored in the system memory. In that case,

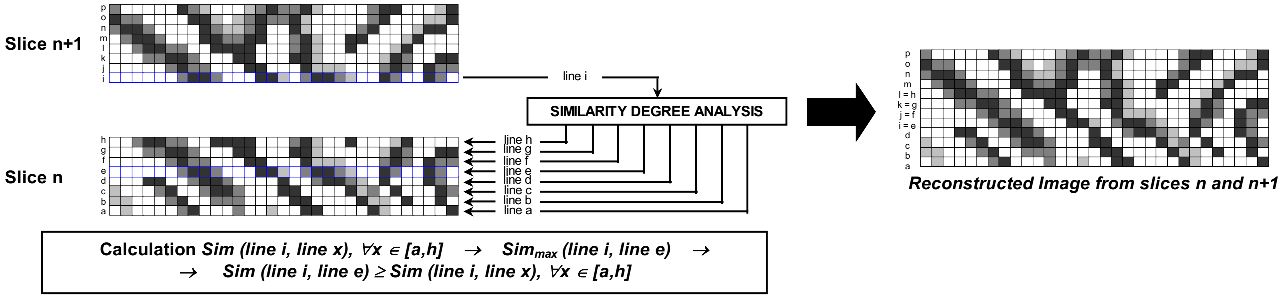
Slice n+1
p
o
n
m
l
k
j
i
line i
SIMILARITY DEGREE ANALYSIS
Slice n
h
g
f
e
d
c
b
a
line h
line g
line f
line e
line d
line c
line b
line a
Calculation Sim (line i, line x), ∀x ∈ [a,h] → Sim_max (line i, line e) →
→ Sim (line i, line e) ≥ Sim (line i, line x), ∀x ∈ [a,h]
p
o
n
m
l = h
k = g
j = f
i = e
d
c
b
a
Reconstructed Image from slices n and n+1

Figure 6. Image reconstruction process of two consecutive acquired slices.

computation must be done after each slice acquisition. The optimal solution has been to use both, the hardware (FPGA) and software (microprocessor) resources of SoC device to implement all the tasks involved in the application, getting as result a good performance fingerprint acquisition system.

B. *Hardware-Software Partitioning*

The first stage in the physical implementation of the system is the partitioning of the different tasks involved in the application. The application flow diagram is shown in figure 7.

Those compute-intensive tasks have been selected to be implemented by hardware in the internal FPGA, whereas the other less costly tasks have became software tasks, executed by the microprocessor. It has been selected as hardware tasks the image acquisition and reconstruction stages, leaving the finger detection and fingerprint image storage as software tasks.

Task 1 allows to detect the presence of a finger on the sensing surface, warning then the system in order to start the acquisition phase. Tasks 2, 3 and 4 are concurrent tasks, and they take place during the slice acquisition sequence. Once the last slice of the fingerprint is acquired, correctly reconstructed and added to the rest of the stored image, the process finishes by going to the final task 5. This one disables the fingerprint acquisition system until a new finger is detected over the sensing surface. A block diagram of the application is shown in figure 8.

C. *Image Acquisition Stage*

The acquisition stage involves the following tasks:

a) handling of the sensor to get the fingerprint slices,

b) storage of the captured slices in a correct way in order to facilitate the concurrent image reconstruction task.

The acquisition core block is responsible for managing the control signals of the sensor. After a system reset, a low frequency (400 kHz) scanning stage of the sensing surface is started by the acquisition controller in order to detect the presence or not of a finger. If no finger is detected, the system keeps in this initial scan phase (standby mode), lowering the total consumption of the module. But once a finger is detected, the acquisition core generates an interrupt to the reconstruction core block, and the slice acquisition sequence starts.

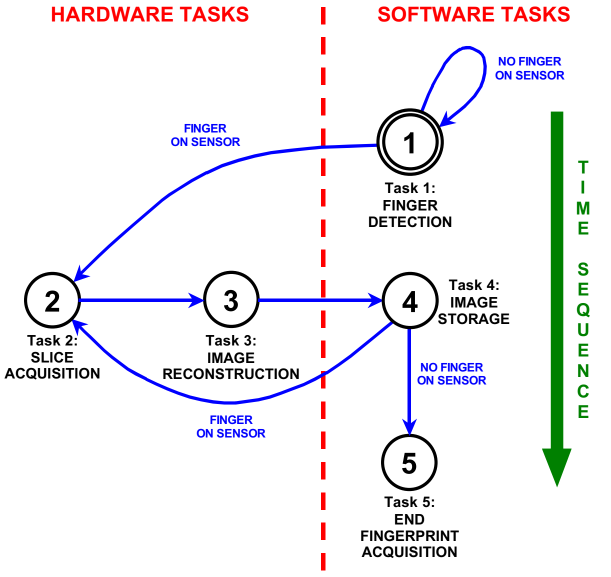

Figure 7. Application flow diagram.

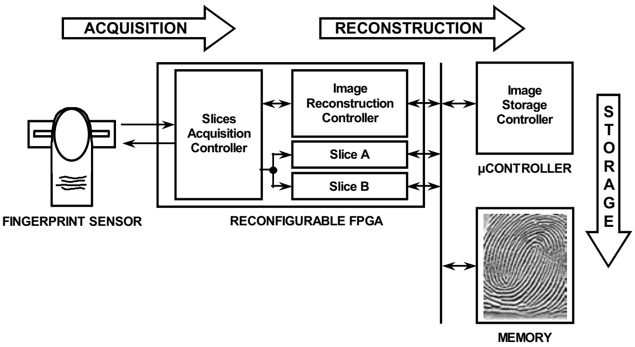

Figure 8. Hardware-software co-design Fingerprint Acquisition System.

The reconstruction core block controls not only the image reconstruction, but also the acquisition so, it gives the start command to the acquisition controller in order to acquire consecutive slices.

In the slice acquisition stage, the scan frequency of the sensor frames keeps at 400 kHz, so the 8 x 280 pixels composing one slice are read in a period of 1124 clocks, that is 2560 µs.

These data, sequentially read from the external sensor, is directly written to an internal memory synthesised on the FPGA. This FPGA memory is split in 2 blocks, corresponding to the capacity of 2 slices (A and B), in order to facilitate the reconstruction task.

Once a complete slice is read, the acquisition core keeps in standby until a new slice acquisition command comes from the reconstruction core block. This is done every 5 ms (slices acquisition rate of 200 slices per second). The acquisition core writes the consecutive coming slices to slice A and B in a sequential way. This working mechanism is done repeatedly until the whole fingerprint is acquired.

D. *Reconstruction on the Fly Stage*

The reconstruction stage is responsible for the following tasks:

a) management of the concurrent acquisition stage,

b) reconstruction of the fingerprint image from the acquired slices,

c) handshaking with the microcontroller in order to allow the image storage process by the microcontroller.

Once the first slice of the image is acquired, the reconstruction phase starts. While the second slice is being acquired, a line comparator analyses the similarity level between the first line of the second slice and every one of the 8 lines composing the first slice, in order to find overlap between consecutive slices. Once the whole second slice is acquired and detected where the overlap is done, an interrupt is generated to the microcontroller. The microcontroller then transfers the overlapped lines to the storage memory.

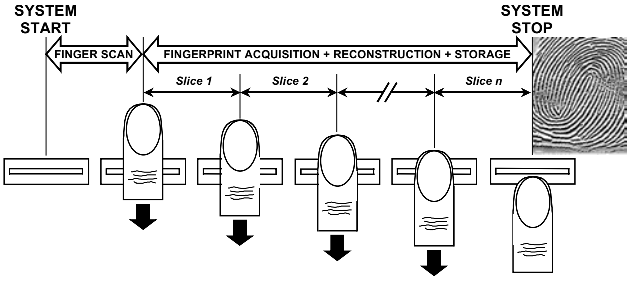

Figure 9. Fingerprint acquisition process.

The acquisition stage is repeated continuously until the finger is taken away from the sensing surface or until the total storage memory is reached. Then, a stop command is transmitted from the microcontroller to the acquisition logic of the FPGA in order to finish the acquisition process.

The fingerprint acquisition time is obviously dependent of the finger sliding speed (or the number of frames overlapped in every consecutive acquisitions), but taking into account a fair sliding speed of the finger, the acquisition, reconstruction on the fly and storage tasks take about 4,52 ms per slice on average (at a system frequency of 25 MHz for the FPSLIC and 400 kHz for the sweeping sensor), what means that it is possible to get good quality fingerprint images at an acquisition frequency of 200 slices per second.

VI. Results, Conclusions and Future Work

After implementing the different blocks of the system, we get the results shown in table 1 and figure 10.

The current technological age walks to the *Embedded Security Systems*: embedded electronics + biometric security to improve the communication reliability and the confidentiality performance of the information in the current networked society.

Table 1.
System requirements and performance.

FingerChip device		
	f_{clk}	400 kHz
	Sensing surface	8 x 280 pixels
	Pixel pitch	50 µm x 50 µm
FPSLIC device (resources used / total resources)		
Memory	Data memory	8753 / 16384 bytes
	Code memory	1907 / 20480 bytes
CPU	f_{clk}	25 MHz
	Percent Load CPU	45%
FPGA	f_{clk}	400 kHz
	Percent Full (Logic)	44%
	# Gate equivalents	144 / 40000 gates
	# LUTs	977 / 4608 LUTs
	# Core cells	912 / 2304 cores
	Percent Full (Memory)	89%
	# Free RAM	2048 / 2304 bytes
System timing		
Task 1	t_1 finger detection	25 µs
Task 2	t_2 slice acquisition	2560 µs
Task 3	t_3 image reconstruction	20 µs
Task 4	t_4 image storage *(mean)*	1940 µs
Slice processing	$t_2 + t_3 + t_4$	4520 µs < 5000 µs
Slice acquisition	200 slices/s	5000 µs

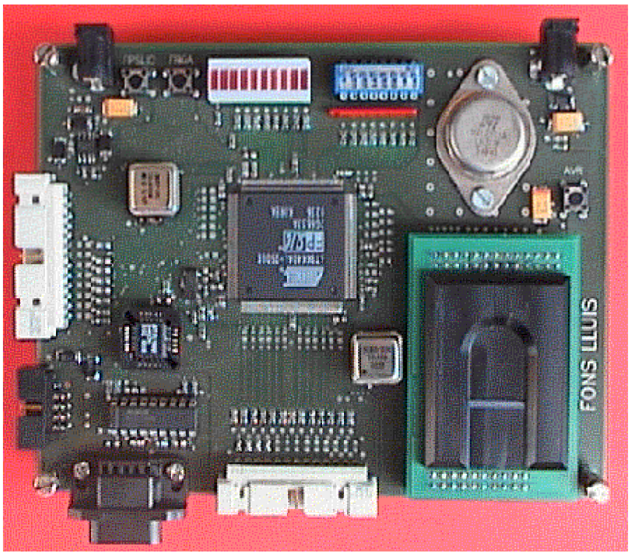

Figure 10. Prototype board developed.

The platform shown in this article permits the hardware-software co-design of medium-low complex systems. The described architecture has provided the authors with a low-cost solution for high performance applications, achieving important savings with respect to the usual implementations of this kind of applications, based on powerful computers executing software tasks at high speed.

It has been detailed the first stage involved in any automated fingerprint identification system. The aim of the authors in their future work is to profit the advantages of reconfigurability performance of the FPGA in order to develop all the steps involved in the recognition process: not only the image acquisition step –already performed–, but also the image enhancement phase, the signature extraction, the signature storage, the biometric matching and the encryption of the verification result.

There already exist the knowledge, the EDA tools and the resources to develop this kind of high performance applications at low cost.

References

[1] A. K. Jain, R. Bolle and S. Pankanti, *Biometrics. Personal Identification in Networked Society*, Kluwer Academic Publishers, 1999.

[2] L.C. Jain, U. Halici, I. Hayashi, S. B. Lee and S. Tsutsui, *Intelligent Biometric Techniques in Fingerprint and Face Recognition*, CRC Press LLC, 1999.

[3] D. Maltoni, D. Maio, A. K. Jain and S. Prabhakar, *Handbook of Fingerprint Recognition*, Springer, 2003.

[4] A. Jain, L. Hong and R. Bolle, "On-Line Fingerprint Verification", *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 19, no. 4, pp. 302-313, 1997.

[5] V. K. Sagar, C. Greening, W. Y. Tan and C. S. A. Leung, "Hardware/Software Co-Design of a Fingerprint Recognition System", *IEE Colloquium on Partitioning in Hardware-Software Codesigns*, pp. 10/1-10/5, 1995.

[6] M. Aberbour, H. Mehrez, F. Durbin, J. Haussy, P. Lalande and A. Tissot, "Design of a System-On-a-Chip for Pattern Recognition", *43rd Midwest Symposium in Circuits and Systems*, Lansing MI, August 8-11, 2000.

[7] The Biometric Consortium, www.biometrics.org.

[8] Atmel Corporation, www.atmel.com.