An Embedded Biometric Sensor for Ubiquitous Authentication

V. Conti
Facoltà di Ingegneria, Architettura e delle Scienze Motorie
Università degli Studi di Enna Kore
Cittadella Universitaria, 94100 Enna, Italy
vincenzo.conti@unikore.it

S. Vitabile
Dipartimento di Biopatalogia e Biotecnologie Mediche e Forensi
Università degli Studi di Palermo, Via del Vespro, 90127, Palermo, Italy
salvatore.vitabile@unipa.it

G. Vitello and F. Sorbello
Dipartimento di Ingegneria Chimica Gestionale Informatica Meccanica
Università degli Studi di Palermo
Viale delle Scienze, Ed. 6, 90128, Palermo, Italy
filippo.sorbello@unipa.it

***Abstract* - Communication networks and distributed technologies move people towards the era of ubiquitous computing. An ubiquitous environment needs many authentication sensors for users recognition, in order to provide a secure infrastructure for both user access to resources and services and information management. Today the security requirements must ensure secure and trusted user information to protect sensitive data resource access and they could be used for user traceability inside the platform. Conventional authentication systems, based on username and password, are in crisis since they are not able to guarantee a suitable security level for several applications. Biometric authentication systems represent a valid alternative to the conventional authentication systems providing a flexible e-infrastructure towards an integrated solution supporting the requirement for improved inter-organizational functionality. In this work the study and the implementation of a fingerprints-based embedded biometric system is proposed. Typical strategies implemented in Identity Management Systems could be useful to protect biometric information. The proposed sensor can be seen as a self-contained sensor: it performs the all elaboration steps on board, a necessary requisite to strengthen security, so that sensible data are securely managed and stored inside the sensor, without any data leaking out. The sensor has been prototyped via an FPGA-based platform achieving fast execution time and a good final throughput. Resources used, elaboration times of the sensor are reported. Finally, recognition rates of the proposed embedded biometric sensor have been evaluated considering three different databases: the FVC2002 reference database, the CSAI/Biometrika proprietary database, and the CSAI/Secugen proprietary database. The best achieved FAR and FRR indexes are respectively 1.07% and 8.33%, with an elaboration time of 183.32 ms and a working frequency of 22.5 MHz.**

KEYWORDS: Self-contained sensor; Biometric identity management; Fingerprints; Ubiquitous authentication; Embedded system;, FPGA rapid prototyping.

I. INTRODUCTION

Ubiquitous and distributed applications are changing the way people communicate, providing services and functionalities, supported by computer networks. Secure access system design is one of the main issues to be considered in ubiquitous and distributed environments [9]. These systems must provide secure access services: this is a serious problem because ubiquitous computing applications typically involve interactions among a large number of entities (e.g. people, server, etc…) across different organizations. Ubiquitous accesses are usually realized through many access-points and a central database [1]. With more details, the main goal of a distributed system is to connect users and resources in a transparent, open, and scalable way. For this reason, one of the fundamental characteristics of distributed systems is its openness. This property is such that each subsystem is open to interaction with other systems, through standard web services protocols which enable distributed systems to be extended and scaled.

Unconstrained entities interaction and uncontrolled information disclosure are the main problems regarding openness of distributed systems, because unauthorized use and information exchange may have extremely grave consequences about security and integrity of the system.

The requirement of trusted access-point [2] involves a greater computational load from applications, because it must provide additional functionalities, for authentication and credentials verification, to guarantee an high security level for each system's access-point [2] [8]. Locally and remote authentication is necessary because people must be able to access services and information from everywhere.

The conventional authentication systems (based on username and password) are not able to guarantee a suitable protection level for the transmitted information. The security user should be the main point of any software application dealing with personal information. Unlike passwords, user

biometric information is unchangeable. Physical and behavioral people characteristics constitute the core of biometric systems: the biometric identity has the advantage to guarantee that only the authorized users have access to available resources and services [9].

In literature many approaches have been proposed and many software systems have been implemented to develop software recognition systems: in [7] a software algorithm for multimodal identification based on fingerprint and iris is proposed. This approach is based on a particular fusion at features level to increase the system performance in terms of accuracy. In [8] an hardware fingerprint recognition system is presented and realized using the Precise Biometrics PB100MC device, as image scanner, and the Celoxica RC1000 board, employing a Xilinx VirtexE2000 FPGA, as fingerprint processing module. In 2004 IBM released a second generation of notebook Thinkpad T42 models [18] equipped with an integrated fingerprint reader produced by UPEK [19]. UPEK TouchStrip is an USB device performing the matching algorithm in hardware: it is a compact CMOS capacitive silicon-based strip sensor (TCS3) for fingerprint acquisition plus a powerful ASIC (TCD4) for fingerprint matching and secure data transfer. However, IBM does not give any information about the database used for the T42 system testing.

In this work, a fingerprint recognizer has been implemented and proposed for a secure biometric identity management system. The main objectives of the proposed biometric sensor are to overcome some limits of the conventional software fingerprint recognition systems, such as user interaction speed and resistance to attacks related to the biometric data transmission and management. With this approach, the proposed system can be considered as a self-contained biometric sensor.

FAR (False Acceptance Rate, related to not authorized users that are admitted) and FRR (False Rejection Rate, related to authorized users that are rejected) indexes have been used to evaluate the performance of the proposed system. Different tests have been performed on three databases: FVC standard database, CSAI/Biometrika and CSAI/Secugen, two proprietary databases: a FAR of about 1% and a FRR of about 8% represents the best trade-off obtained.

The paper is organized as follow. Section II illustrates the problems related ubiquitous authentication and security. Section III describes the proposed embedded sensor. Section IV illustrates each phase of fingerprint processing chain. Section V presents the experimental results in terms of elaboration times and recognition rates. Finally, section VI reports the conclusions of this work.

II. UBIQUITOUS AUTHENTICATION AND SECURITY

Conventional authentication methodology, based on username and password, is the easiest people authentication method to implement and to use, but it is not sufficient for these applications, as distributed systems, that need high data protection. Many limitations can be found in this approach, such as easiness to forget, lose and intercept the username or the password, therefore it aren't suitable for distributed systems. The most secure and effective personal authentication and identity management method involve the verification of a unique and personal biometric characteristic. Identity management is related to the registration, storage, protection, issuance and assurance of a user's personal identifier in an electronic environment.

A secure infrastructure is necessary for ubiquitous authentication, where all people could be reliably authenticated. Trustiness is an essential requirement for these systems and networks, whose transactions can be performed without any compromise. Critical IT services supplied to people (e.g. banking, where credit card accounts or other personal information cannot be shared or stolen) need a high grade of security. An ubiquitous authentication system can be seen as a specialized sensor that reduces the points-of-attack of conventional authentication systems and that gives the capability to authenticate people in secure manner, across applications and networks.

Software and hardware systems for fingerprints recognition represent alternative solutions of strong and robust user authentication. In reference to the vulnerability, a recognition system can be considered secure and trusted only if it withstands some typical attacks [1]: Replay Attacks (due to the replication of the information elaborated during the authentication process), Communication Attacks (evaluated in terms of resistance to the information interception), Database Attacks (regarding the information manipulation of the contained in the system database).

A possible choice could be the implementation of an embedded database, since biometric information are encrypted and stored in the memory, tamper-resistant device. In addition, the biometric sensor has on board all the information needed to perform the whole user authentication task. No sensible biometric information is transmitted between client and server, or networked workstations before the positive user authentication.

III. THE PROPOSED EMBEDDED SENSOR

In this work the authors present a fingerprint based embedded sensor. Both the enrollment phase and the authentication phase have been developed for sensor employment in real ubiquitous environments. Fingerprint processing as well as fingerprint-templates matching are on-board executed without any information transmission before a positive authentication. The proposed sensor acquires a fingerprint image, processes it and, in matching phase, gives a similarity index used for user authentication. Considering the functionalities of the system components, three main modules can be identified [8]: User Interface Module (UIM), System Processing Module (SPM), Sensor Acquisition Module (SAM). The UIM allows user to interact with the enrollment and authentication functionalities provided by the system. The SAM deals with fingerprint image acquisition. The SPM, the FPGA-based fingerprint processing engine, implements the

whole recognition chain and the cryptographic capabilities of the sensor.

In Fig.1 the UIM, the SAM, and the SPM with their interconnections are depicted: using the functionalities offered by the UIM, the sensor through the SAM acquires a fingerprint image. Subsequently the acquired image is sent to the SPM using both the host expansion bus and the host PCI bus.

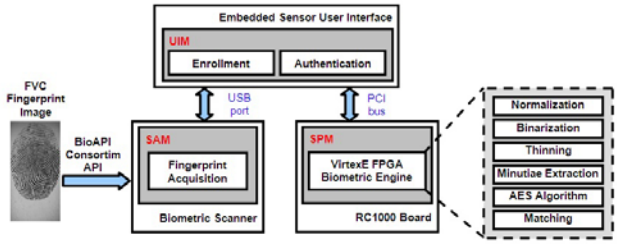

Fig. 1. The proposed system modules: the User Interface Module (UIM), the System Processing Module (SPM), the Sensor Acquisition Module (SAM) and their main interactions.

The SPM prototype has been developed on the Celoxica RC1000 board equipped with a 2M gates Xilinx VirtexE2000 FPGA. SPM communications use only the host PCI bus and its clock has been set to 22.5 MHz in order to guarantee the correct data exchange between FPGA and board RAM that is used to store the encrypted fingerprint templates. Exploiting the high data parallelism of the application domain, processing algorithms have been parallelized and fingerprint processing phases have been pipelined to decrease system execution time.

A. The Self-Contained Fingerprint Sensor

The main objectives of the proposed sensor are to overcome some limits of the conventional software fingerprint recognition systems (user interaction speed and attacks resistance related to biometric data transmission and management). The proposed fingerprint recognizer can be seen as a self-contained biometric sensor. The self-contained sensor has been realized using a fingerprint image scanner and the Celoxica RC1000 board [13], as fingerprint processing engine. For this type of biometric sensors, one of the most important phases is the minutiae extraction and their storage in the board. Fingerprint minutiae extraction is a complex job, depending on many factors (a software implementation, from the point of view of the elaboration times, constitutes a bottle-neck) thus the fingerprint processing chain is implemented and executed on a FPGA based device. Besides, to increase security, the biometric templates are encrypted and stored on the board RAM. With this approach, the biometric sensor will contain all the information/data needed to perform user authentication without information transmission through the network or server/workstation [4][15]:

- the FPGA allows to resolve the safety problems in the treatment of the biometric characteristics (Replay Attack);
- the AES (Advances Encryption Standard) used to encrypt/decrypt the biometric signatures, avoid to transmit plain-text information, making unusable the biometrics greatness intercepted (Communication Attack);
- the system interacts with the embedded database, encrypted and stored in the FPGA memory, so that the problem of unauthorized access to the biometric signatures (Database Attack) can be exceeded.

Besides, the choice of a FPGA implementation exceeds software system general problems, such as performance and response time.

IV. FINGERPRINT RECOGNITION PHASES

A. FPGA Fingerprint Preprocessing

Normalization: it reduces the data-noise before image is submitted to thinning and minutiae extraction modules. The normalization allows to the grey levels of original image (Fig.2a) to converge around an average value with a desired variance (Fig.2b).

Binarization: it gives out an image where pixels assume a binary value (Fig.2c). The binarization is performed applying two different elaborations to the input image: an average filter and a thresholding operation with two different thresholds.

Thinning: it reduces the ridges thickness to the unitary value (Fig.2d), using the Zhang-Suen algorithm [10]. This algorithm gives the opportunity to a parallel implementation with a two stage pipeline. For the realization of the thinning algorithm on FPGA, a 3x3 mask has been used in order to implement the two steps pipeline.

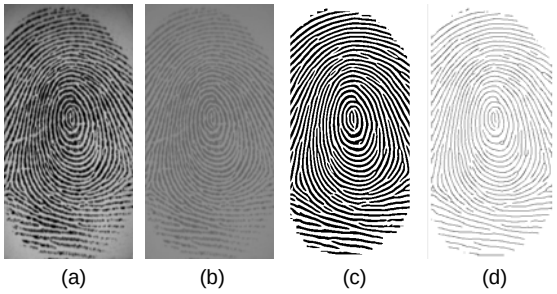

Fig. 2. FVC database fingerprint images: original image (a), normalized image (b), binarized image (c), and thinned image (d).

B. FPGA Fingerprint Minutiae Extraction

For the minutiae extraction phase the Tico-Kuosmanem algorithm [11] has been used. In our implementation, two further procedures have been added to traditional algorithm implementation: the first step asks for analysis and individualization of minutiae type (i.e. ending and bifurcation points), the second step is necessary to erase the false minutiae. The hardware implementation takes advantage of the nature of the used algorithm: pipeline stages have been used

for minutiae extraction. Fig.3 shows the fingerprint minutiae extraction phase. After, the biometric template is created from these extracted points.

For security constraints, the biometric templates are encrypted using AES (Advanced Encryption Standard) algorithm [12].

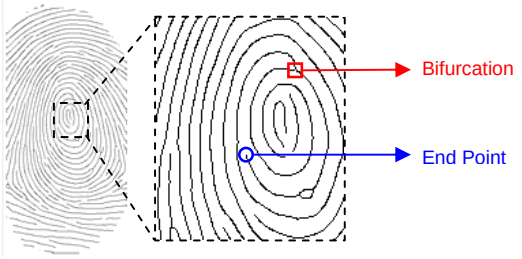

Fig. 3. Example of detected minutiae.

C. *FPGA Fingerprint Template Matching*

Several algorithms are available for fingerprint template matching [6]. Those based on pattern matching give the best performance on hardware, due their possibility of parallel implementation.

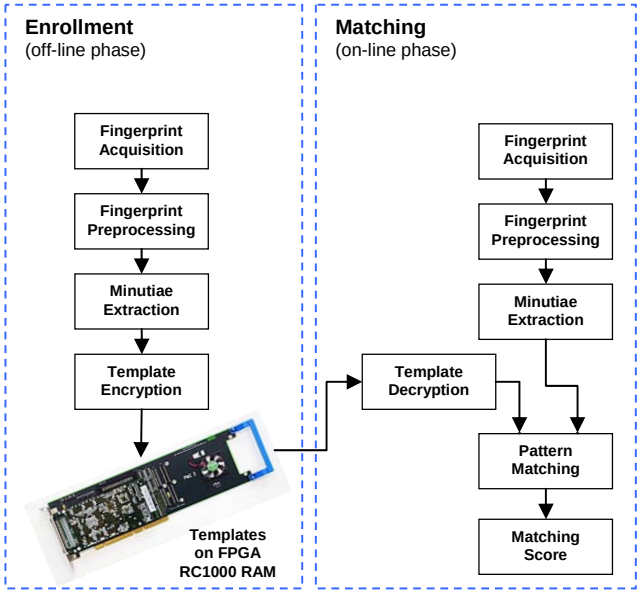

Fig. 4. Enrollment and authentication phases of the prototyped embedded self-contained sensor.

In the procedure that brings the user to its authentication, two phases can be detected (Fig.4):

- off-line phase: user fingerprints are acquired and processed for creating the biometric templates.
- on-line phase: the registered user is authorized to access system services and resources after a positive authentication involving the stored fingerprint templates and the on-line acquired item.

The algorithm executes a pattern matching task between two biometric templates, lining-up the patterns with roto-translation transformation. As result, the algorithm gives a similarity score among two fingerprints.

V. EXPERIMENTAL RESULTS

This section illustrates features and results of the prototyped sensor. The achieved experimental results, in terms of resources analysis, times analysis, performance analysis and recognitions rates are also shown.

A. *Hardware Components*

The FPGA based board used for sensor prototyping is the Celoxica RC1000 board [13], an internal board on PCI bus, equipped with the Xilinx VirtexE2000 FPGA, 8MB of RAM and a programmable clock. The two used fingerprint scanners are the Secugen Hamster FDP02 [16] and the Biometrika FX2000 [17]. These scanners are compatible with BioAPI Consortium libraries [5], leaving ample room for the developing of the communication protocol between scanners and processing engine.

B. *Execution Times*

The proposed self-contained sensor takes advantage of FPGA technologies previously described. Table I illustrates the elaboration times required by each single task of the authentication process, with a working frequency of 22.5 MHz. The fingerprint image is acquired with Secugen Hamster scanner, and transferred to the FPGA processing engine.

Table I. Elaboration times of each task with the Secugen Hamster scanner. The working frequency is 22.5 MHz.

Processing Task	Processing Time (ms)
Normalization	5.24
Binarization	4.36
Thinning	78.02
Minutiae Extraction	27.4
AES Encryption	29.6
AES Decryption	31.2
Matching	7.5
TOTAL TIME	**183.32**

C. *Resources analysis*

The development environments used in the prototyping phase were the Celoxica DK2 [14] and Xilinx ISE [15]. Table II illustrates the FPGA resources required by every processing task.

Table II. Resources used by each processing task.

Processing Task	Slice Number	Slice (%)	LUT Number	LUT (%)
Normalization	91	0.47	102	0.26
Binarization	113	0.59	95	0.25
Thinning	358	1.86	442	1.15
Minutiae Detection	12491	65.06	22518	58.64
AES	5967	31.08	13538	35.26
Matching	129	0.67	109	0.28

Table III illustrates the global percentages of used FPGA resources. The results are always referred to fingerprint images acquired by Secugen Hamster scanner. Similar results were obtained using the Biometrika FX2000 scanner.

Table III. The used FPGA physical resources in terms of GCLKs (global FPGA clock), GCLKIOBs (clock for I/O management), IOBs (I/O blocks), SLICE (logical cells contained in the CLBs - Configurable Logic Block), LUTs (Look-Up Table used as Boolean function generator).

Resource Type	Total Resource	Used Resource	Use Percentage
GCLKs	4	2	50.00
GCLKIOBs	4	1	25.00
IOBs	404	273	67.57
SLICEs	19200	19198	99.99
LUTs	38400	37031	96.43

D. Sensor Storage Capabilities of User's Templates

The embedded biometric sensor uses the RC1000 board RAM to store and manage user biometric identity. With more details, one memory bank has been used for temporary storage process required by fingerprint processing tasks, while the remaining 3 memory banks (6MB) have been used for to store user's biometric templates. Each user template requires 512 byte, considering a variable number of templates. Table IV shows the maximum number of users that can be enrolled on the sensor.

Table IV. Maximum number of user templates stored in the board memory.

Template Number (for each user)	Sensor Storage Capability (number of users)
2	6144
3	4096
4	3072

E. Recognitions Rates

System recognition performance has been evaluated through FAR and FRR indexes. An ideal recognition system would have FAR and FRR values equal to zero. However, in a real system, these indexes will be different from zero. A good processing strategies aims to reduce authentication faults in terms of false accepted users and false rejected users. In order to obtain a better validation of FAR and FRR indexes different tests have been performed on three databases:

- FVC2002/DB2 database is composed of 80 fingerprint images, acquired from 10 individuals (8 fingerprints for each individual). The image dimensions are 296x560 pixels obtained from the scanner Biometrika FX2000.
- CSAI/Biometrika database is a proprietary database composed of 365 fingerprint images of 73 individuals (5 fingerprints for each individual). The image dimensions are 296x560 pixels obtained from the scanner Biometrika FX2000 [17].
- CSAI/Secugen database is a proprietary database composed of 352 fingerprint images of 88 individuals (4 fingerprints for each individual). The image dimensions are 300x260 pixels obtained from the scanner Secugen Hamster FDP02 [16].

Table V shows FAR and FRR recognition rates obtained with the performed tests on the above described databases. Firstly, the prototyped fingerprint recognizer has been tested using the FVC database, necessary to obtain an evaluation on a standard database of the proposed approach.

Table V. Recognition results of the implemented sensor on the tested databases.

Database	FAR (%)	FRR (%)
FVC2002/DB2	1.52	20.35
CSAI/Biometrika	0.73	9.21
CSAI/Secugen	1.07	8.33

Subsequently, two different tests have been performed of the CSAI/Biometrika and CSAI/Secugen proprietary databases: in these last two cases, the system recognition performance is substantially improved respect FVC database test. This improvement is due considering that FVC is an official database used expressly to perform comparable tests on biometric systems. With more details, for the indexes calculation, some thresholds of coincident minutiae have been fixed: these thresholds define how much similar have to be two biometric signatures to give a positive matching. Also, has been considered the number of biometric templates with which to perform the comparison. This means that during the matching the biometric template obtained by the on-line fingerprint has been compared with 2, 3 or 4 templates stored in the sensor database. To increase the clearness of the proposed approach, the following Table VI shows the FAR-FRR pairs obtained on the CSAI/Secugen database, considering different templates and minutiae number.

The relative Fig.5 shows the FAR and FRR curves when fingerprint matching is performed using 2 fingerprint templates. A trade-off is necessary for optimal choice of FAR and FRR indexes. Table VI shows a possible optimal choice of

the FAR and FRR pair (FAR=1.07% and FRR=8.33%) for the proposed system, obtained requiring the 95% of matched minutiae and 2 templates. The experimental trials involving the highest number of fingerprint templates (4) denote a low FAR but a high and unfeasible FRR

Table VI. FAR and FRR indexes with different percentage of minutiae and different number of enrolled user templates.

Percentage Minutiae	**93%**		**95%**		**97%**	
Template Number	FAR (%)	FRR (%)	FAR (%)	FRR (%)	FAR (%)	FRR (%)
2	1.68	7.29	**1.07**	**8.33**	0.98	11.46
3	1.12	17.71	0.78	22.92	0.71	26.04
4	0.87	40.63	0.60	46.88	0.41	52.08

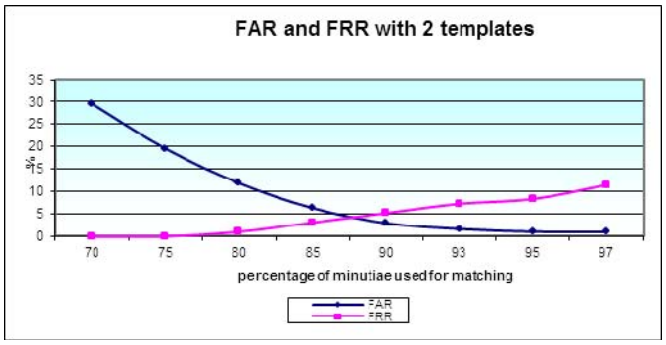

Fig. 5. FAR and FRR curves when fingerprint matching is performed using 2 fingerprint templates.

VI. CONCLUSION

In this work the study and the implementation of a fingerprints-based embedded biometric system for personal ubiquitous authentication and identity management has been proposed. An ubiquitous environment needs many authentication sensors for users recognition and their secure access to services and resources. In order to reach the objectives related to both security levels and performance in ubiquitous environments, the authors have designed and prototyped a self-contained sensor based on FPGA technologies. The entire encrypted user database is stored on the board RA8M. Each user optimized biometric template requires only 512 bytes, so a single board can store more than 6000 user biometric templates. The embedded sensor prototype has been tested on three databases: the FVC2002 reference database, the CSAI/Biometrika proprietary database, and the CSAI/Secugen proprietary database. System performance has been evaluated using FAR and FRR indexes. The best achieved FAR and FRR indexes are respectively 1.07% and 8.33%, with an elaboration time of 183.32 ms and a working frequency of 22.5 MHz. The low working frequency suggests interesting considerations for the employment on the embedded recognizer in portable devices, since one of the techniques used to reduce device power consumption is to have a low working frequency with an adequate processing time for the device.

REFERENCES

[1] Hui Liu; Cai-Ming Zhang; "Research on Use of Distributed Authentication in Pervasive Computing", 1st International Symposium on Pervasive Computing and Applications (SPCA06), Pages:571-574.

[2] Yin, Shuxin; Ray, Indrakshi; Ray, Indrajit; "A Trust Model for Pervasive Computing Environments", 2nd International Conference on Collaborative Computing, 2006, Pages:1-6.

[3] Sailer, R.; Giles, J.R.; "Pervasive authentication domains for automatic pervasive device authorization", 2nd IEEE Conference on Pervasive Computing and Communications Workshops Pervasive Computing and Communications Workshops, 2004, (PerCom 2004), Pages:144-148.

[4] UK Biometrics Working Group (BWG): "Biometrics Security Concerns" (2003)

[5] BioAPI Specification Version 1.1, March 16, 2001 Developed by The BioAPI Consortium http://www.bioapi.org.

[6] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, Handbook of Fingerprint Recognition. New York: Springer-Verlag, 2005.

[7] V. Conti, C. Militello, F. Sorbello, S. Vitabile. "A Frequency-based Approach for Features Fusion in Fingerprint and Iris Multimodal Biometric Identification Systems", IEEE Transactions on Systems, Man, and Cybernetics (SMC) Part C: Applications & Reviews, Vol. 40 issue 4, pp. 384-395. 2010, DOI:10.1109/TSMCC.2010.2045374

[8] S. Vitabile, V. Conti, C. Militello, F. Sorbello, "A Self-Contained Biometric Sensor for Ubiquitous Authentication", IEEE International Conference on Intelligent Pervasive Computing (IPC 2007), 2007, ISBN/ISSN: 0-7695-3006-0, pp. 289-294.

[9] C. Militello, V. Conti, S. Vitabile and F. Sorbello, "Embedded Access Points for Trusted Data and Resources Access in HPC Systems", The Journal of Supercomputing, Springer Netherlands Publisher, 2011, ISSN 0920-8542, Vol. 55, N° 1, pp. 4 – 27, (ISSN Online 1573-0484), DOI:10.1007/s11227-009-0379-1

[10] T.Y. Zhang, C. Y. Suen: " A fast parallel algorithm for thinning digital patterns", Comm. ACM, Vol. 27, Issue 3, Pages: 236-239, 1984.

[11] M. Tico, P. Kuosmanen: "An Algorithm for Fingerprint Image Postprocessing", IEEE Transactions On Pattern Analysis And Machine Intelligence, pp.1735-1739, 2000.

[12] J. Daemen and V. Rijmen AESs proposal: Rijndael. citeseer.ist.psu.edu/daemen98aes.html.

[13] "RC1000 Hardware Reference Manual", Celoxica Ltd. web site: http://www.celoxica.com.

[14] "DK User Guide". Celoxica Ltd. web site: http://www.celoxica.com.

[15] P.Ambalakat, "Security of Biometric Authentication Systems", 21st Computer Science Seminar. SA1-T1-1. Page 2, www.rh.edu/~rhb/

[16] Secugen Corporation web site: http://www.secugen.com/

[17] Biometrica srl web site: http://www.biometrika.it/

[18] IBM Thinkpad T42 http://www.thinkwiki.org/wiki/Integrated_Fingerprint_Reader.

[19] UPEK TouchStrip http://www.upek.com/support/pdf/UPEK_flyer_TCS3_TCD4.pdf