The Knowledge Engineering Review, Vol. 30:2, 201–219.
doi:10.1017/S0269888914000307

Biometric sensors rapid prototyping on field-programmable gate arrays

VINCENZO CONTI[1], CARMELO MILITELLO[2], FILIPPO SORBELLO[3] and SALVATORE VITABILE[4]

[1]*Facoltá di Ingegneria, e Architettura, Università degli Studi di Enna KORE, viale delle Olimpiadi, 94100, Enna, Italy;*
e-mail: vincenzo.conti@unikore.it;
[2]*Istituto di Bioimmagini e Fisiologia Molecolare – Consiglio Nazionale delle Ricerche (IBFM-CNR), UOS Cefalu', C.da Pietrapollastra-Pisciotto – 90015 Cefalu' (PA), Italy;*
e-mail: carmelo.militello@ibfm.cnr.it;
[3]*Dipartimento di Ingegneria Chimica, Gestionale, Informatica, Meccanica, Universita' degli Studi di Palermo, 90128 Palermo, Italy;*
e-mail: filippo.sorbello@unipa.it;
[4]*Dipartimento di Biopatalogia e Biotecnologie Mediche e Forensi, Universita' degli Studi di Palermo, via del Vespro, 90127 Palermo, Italy;*
e-mail: salvatore.vitabile@unipa.it

Abstract

Biometric user authentication in large-scale distributed systems involves passive scanners and networked workstations and databases for user data acquisition, processing, and encryption. Unfortunately, traditional biometric authentication systems are prone to several attacks, such as Replay Attacks, Communication Attacks, and Database Attacks. Embedded biometric sensors overcome security limits of conventional software recognition systems, hiding its common attack points. The availability of mature reconfigurable hardware technology, such as field-programmable gate arrays, allows the developers to design and prototype the whole embedded biometric sensors. In this work, two strong and invasive biometric traits, such as fingerprint and iris, have been considered, analyzed, and combined in unimodal and multimodal biometric sensors. Biometric sensor performance has been evaluated using the well-known FVC2002, CASIA, and BATH databases.

1 Introduction

Large-scale distributed systems enable the sharing and aggregation of geographically distributed resources by different organizations with distinct owners, administrators, and policies. In that context, it is arguably required to investigate novel methods and techniques to enable secure systems, data, and resources access (Oey *et al*., 2010). Large-scale distributed systems use several distributed access points for users authentication. Traditional access points are composed of passive scanners, networked workstations, and databases for user data acquisition, processing, and encryption. Authentication systems run on trusted servers to match acquired information against the corresponding stored templates.

However, authentication procedures, based on the simple username–password pair, are insufficient to provide a suitable security level for those applications requiring high data and services protection. Biometric-based authentication systems represent a valid alternative to conventional approaches. Biometric authentication systems, using invasive physiological characteristics, have become popular, mostly for their high capabilities of discrimination (selectivity) to prevent unauthorized access to systems, data, and resources. On the other hand, the immutability of these features makes extremely strong and robust authentication systems design possible. However, biometry can be a severe weakness: if biometric data

is stolen, it will be permanently compromised and it cannot be replaced, unlike IDs, passwords, and certificates.

Unfortunately, software biometric authentication systems are prone to several attacks, such as Replay Attacks, Communication Attacks, and Database Attacks (UK Biometrics Working Group (BWG), 2003). The main objective of an embedded sensor is to overcome the security limits of the conventional software recognition systems, hiding the most common attack points of a biometric authentication system (Ambalakat, 2005). The use of field-programmable gate arrays (FPGA) technology overcomes the security issues in the biological data management phase (*Replay Attacks*), as biometric traits processing and matching are performed into the embedded sensor. In addition, the common attacks related to the biometric data transmission between modules are cut out. The use of cryptography (biological templates are ciphered using the Advanced Encryption Standard (AES) encryption algorithm; Mali *et al*., 2005) avoids the transmitting of clear information between system modules (*Communication Attacks*). Finally, the tamper-resistant smartcard provides a secure environment to store biometric templates. In addition, no distributed or centralized database is needed with smartcards, avoiding the presence of databases-linked points of failure (*Database Attack*). Concerning the analysis on biometric authentication system security presented in Ambalakat (2005), embedded biometric sensors overcome the security limits linked to the data transmission tasks between scanner and feature extractor, and between feature extractor and matcher (Militello *et al*., 2011). Biometric sensors could be integrated by the needed solutions for keys management and distribution, involving decentralized certification authorities (CAs), as proposed and evaluated in Nielsen and Hamilton (2005), Michener and Acar (2000), and Niu *et al*. (2009).

In this paper, a number of significant developed and tested unimodal and multimodal biometric-embedded sensors are presented. Two strong and invasive biometric traits, such as fingerprint and iris, have been considered, analyzed, combined, and compared. The presented processing approaches can be divided into two broad groups: micro-features-based systems and macro-features-based systems. Embedded sensors can be further classified on the basis of its working domain, involving the spatial or frequency biometric traits encoding. Unimodal biometric sensors, operating on a single biometric feature (fingerprint or iris) are presented and described. Moreover, multimodal biometric systems and related fusion strategies are presented and developed as alternative approach. Multimodal sensors overcome issues and limits of unimodal sensors, as captured data are often affected by noise, distinctiveness ability, that is, biometric features have not the same distinctiveness degree, and lack of universality, that is, some people do not have the biometric feature which a system might allow.

Biometric sensors have been prototyped using two FPGA-based boards (Mentor Graphics website). The RC1000 board, equipped with a Xilinx Virtex-E FPGA, is installed on a generic PCI workstation. The stand-alone RC203E board, equipped with a Xilinx Virtex-II FPGA, has several I/O interacting devices. Finally, the availability of software development environments (Mentor Graphics website; Xilinx website) and algorithm-like hardware description language (Mentor Graphics website) allow the fast development of FPGA-based sensors. Biometric sensors are based on fingerprint and/or iris processing and their performance has been evaluated using the well-known standard literature databases: the FVC2002 database (BATH Iris Database website) for fingerprint authentication systems, the CASIA (Chinese Academy of Sciences Institute of Automation) and BATH (BATH Iris Database website) databases for iris authentication systems.

The paper is organized as follows. Section 2 introduces the authentication issue in large-scale systems. Section 3 describes the presented embedded biometric sensors. Section 4 shows the experimental results in terms of accuracy, used resources, and execution times. Section 5 deals with the comparison of the state-of-the-art solutions. Finally, Section 6 reports the conclusions of this work.

2 Authentication in large-scale systems

User authentication in large-scale systems is related to two big issues: (i) secure authentication techniques for systems, data, and resources authorized access; (ii) decentralized authentication and authorization authorities for keys and certificates management. The first issue involves the development of trusted and

strong biometric-based authentication systems, servicing millions of clients. The second issue is related to the development of decentralized and shared public key infrastructures (PKI).

2.1 Biometric authentication

Authentication procedures, based on the simple username–password approach, are insufficient to provide a suitable security level for those applications requiring a high level of identity, data, and services protection. Biometric-based authentication systems represent a valid alternative to conventional approaches for identity management and personal authentication (Snijder, 2006). In those systems, user recognition is based on one or more information comparison, derived from physical or behavioral traits, such as fingerprints, face, iris, voice, hand, or signature.

A trusted biometric authentication system has to reduce the point-of-attacks in the recognition chain (Ambalakat, 2005) and has to perform secure user authentication (BWG, 2003). For example, a critical problem in biometric systems is the biological template storage: a centralized database can be intercepted and subjected to external attacks. In reference to the vulnerability, a biometric system can be considered trusted only if it withstands some typical attacks, such as:

1. Replay Attack: it is related to the reply of the fingerprint characteristics involved in the authentication process.
2. Communication Attack: it is valued in terms of resistance to the interceptions of the biometrics information.
3. Database Attack: it concerns the manipulation of the biological templates contained in the database.

How can the security of a biometric recognition system be improved? There comes a time in the development of any biometric recognition system where it becomes increasingly difficult to achieve better performance from a given biometric identifier. The need to explore other sources for improvement becomes a practical necessity. The integration approach to improve performance can take any number of different forms.

One could combine biometric schemes with non-biometrics-based schemes. Cryptography techniques can sensitively increase the potentiality offered by biometric authentication systems. As example, the AES is a very robust cryptographic algorithm (Mali *et al*., 2005). Using AES no clear biometric information between modules is exchanged. On the other hand, the design and use of embedded sensors make possible the whole biometric processing chain to be implemented in the hardware device, so no attacks in the data transmission phase, that is, between scanner and feature extractor, between feature extractor and matcher, are allowed (Ambalakat, 2005). The most secure solution is to manage and process keys and biometric traits on secure, self-contained hardware platforms, as external and less-trusted system components can conduct operations involving session-specific secrets (Militello *et al*., 2011).

The implementation of a biometric-based embedded sensor for user authentication is also an interesting and feasible solution for large-scale systems, as the embedded sensor performs the entire elaboration steps, so that all critical information (i.e. biometric data and cryptographic keys) are securely managed inside a common tamper-resistance device, without any data loss (see Figure 1). In addition, smartcard-based technology provides tamper-resistant storage devices that can improve the security degree of a biometric authentication system (Militello *et al.*, 2011). The use of smartcards, storing the biometric descriptor, and secure keys allows:

1. Control and security: the smartcard guarantees the full control of the transferred data, securing each transaction. No smartcard content access is permitted without the required rights (access conditions).
2. Offline and distributed databases: each user owns its biometric information, keys, certificates, and digital signatures (stored into the smartcard). This decreases the risk of data theft, data tampering, and data spoofing, which are some of the main problems in centralized databases-based approaches.

2.2 Smartcard and cryptography

Large-scale systems need strong procedures to protect data and resources access from unauthorized users. According to a specific target application, the basic purpose of a recognition system is to automatically discriminate between subjects in a reliable and dependable way.

As shown in Figure 2, in the architecture of smartcard framework the software application can directly communicate with the operating system (OS). The OS provides low-level communication functions

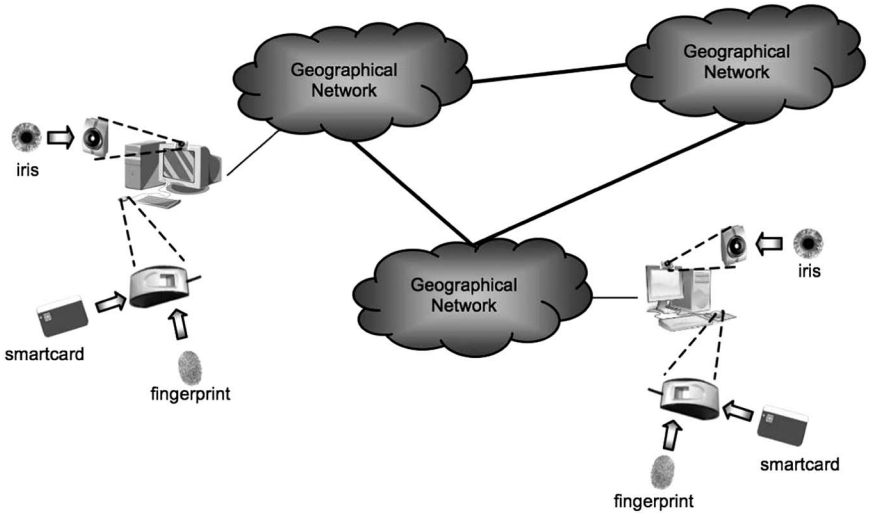

Figure 1 A large-scale system with biometric-embedded sensors for user authentication

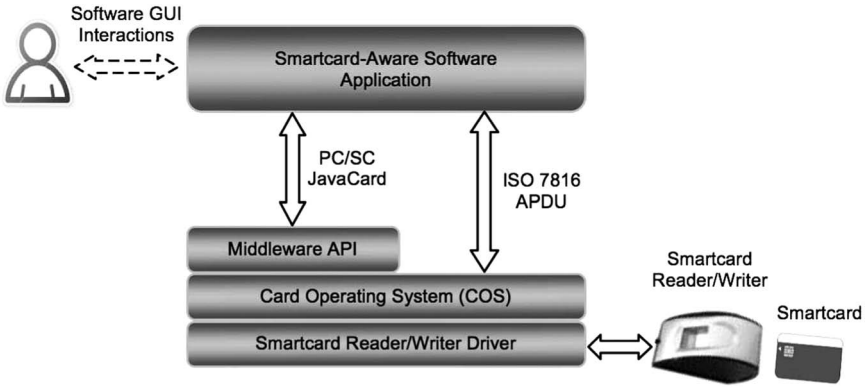

Figure 2 A common architecture of the smartcard framework

(ISO7816), or uses a middleware for mapping its low-level functions with high-level functions, according to the available standards (PC/SC, JavaCard, etc.). The card operating system implements the functionalities offered by a smartcard: its primary objective is the secure and efficient smartcard memory resource management. Smartcard resource access from an external application is directly managed (permissions management) by the OS.

Smartcard and cryptography are closely linked. Although cryptography provides techniques to assure information reservation, nevertheless, it introduces a weak point: the difficulty to protect keys, descriptors, and so on. The smartcard is an adequate, tamper-resistant device to protect reserved data, because it allows the on-board execution of the main cryptographic algorithms without exposing them. For those characteristics, smartcards are used for critical procedures of authentication systems such as user credentials storage.

Smartcard access is subordinated to a PIN verification procedure. After that, the stored user credentials are used for performing authentication.

To preserve the contained data, the smartcard offers two protection levels: the logical level and the physical level. The logical protection level is managed by the smartcard OS. A cryptographic coprocessor equipped smartcard provides a procedure, technically called challenge-response, to get its memory access permission. The above procedure ensures the trustworthy data transmission, implementing secure transactions, and protecting data stored.

The physical protection level is directly managed by smartcard microchip manufacturers. They develop and implement complex EEPROM protection mechanisms making smartcard content reading extremely difficult and expensive. The above protections could be broken through invasive attacks (power analysis, Kocher *et al*., 1999; timing analysis, Kocher, 1999; and electromagnetic analysis, Agrawal *et al.*, 2002). To oppose these attacks, microchip manufacturers use shielding techniques or alarm systems that, in case of violation, erase the EEPROM contents and block the microprocessor. However, the degree of protection can be further enhanced by encrypting the EEPROM contents.

In our sensors the challenge-response procedure with AES data encryption is used (Mali *et al.*, 2005). It is a symmetric key cryptographic algorithm that, for its characteristics, can be easily implemented on hardware architectures. AES uses several matrixes, called S-Box, to implement the transformations. The encryption process is divided in rounds: in each round (except the first one and the last one) the following functions are performed:

1. SubBytes: nonlinear substitution of bytes according to a specific table.
2. ShiftRows: bytes shift of a number of positions dependent from the byte position.
3. MixColumns: linear combination of the byte, considering a column at time.
4. AddRoundKey: combination between the byte and the round key.

In the decryption process the same steps are performed but using the inverse transformations. Further details on the AES algorithm can be found in Mali *et al.* (2005).

However, the smartcard device used in large-scale systems introduces several weak points related to the distribution and the protection of keys, descriptors, and so on. Different solutions for keys management and distribution, involving decentralized CAs, have been proposed and evaluated (Michener & Acar, 2000; Nielsen & Hamilton, 2005; Niu *et al.*, 2009).

2.3 Keys management and distribution

Information and communication technologies (ICT) provide advanced services in large-scale and heterogeneous systems, requiring strong security procedures to protect data and resources access from unauthorized users. Trusted authentication requires a secure infrastructure, where all people could be reliably authenticated. Trustiness is an essential requirement when transactions must be executed without limits and compromises. Critical ICT services supplied to people (e.g. e-commerce or e-banking services) need a high level of security. In Niu *et al.* (2009), an architecture for large-scale storage system implementing a decentralized authentication and authorization schema is proposed. In a decentralized security system, each user and component (e.g. the storage device and metadata server) has a unique identifier *ID*. The user can directly interact with any device in the network by using a single identity certificate without a centralized security server. However, capability-based security solutions have aimed to rapidly authenticate and authorize I/Os, but leave user authentication to different security infrastructures.

The main problem of encrypted keys management is the key generation and distribution process. In 1998, the United States Department of Defense (DoD) investigated the use of public key technology implementing a pilot PKI (Nielsen & Hamilton, 2005). Successively, the DoD has successfully issued digital certificates on common access cards to over 85% of its 3.5 million user population. The DoD PKI consists of a single Root CA and multiple subordinate CAs. The Root CA only issues subordinate CA certificates. Subordinate CAs issue five types of certificates: identity, signature, encryption, component, and code signing. All private keys associated with encryption certificates are first, escrowed to the certificate issuance. In addition, the DoD must manage user smartcard migration issues. Using the smartcard space, the solution proposed in Nielsen and Hamilton (2005) would enable users to perform card maintenance, such as certificate update, from their own workstations instead of returning to an issuance station. However, all DoD users will not be able to take advantage of these new capabilities until all cards have been replaced through normal expiration.

Another solution for keys generation and distribution has been proposed in Michener and Acar (2000). The authors develop their approach on the group-security-domain (SD) paradigm. An SD is a collection of

systems (servers, devices, and so on) that share a common set of keys and are linked to an administered network. High-integrity secure communication systems typically rely on dedicated and secure key-management servers that are not administered as part of the overall network. Their approach divides the network into smaller virtual partitions (domains). They manage keys as part of a large-scale network that spans different geographic locations and contains thousands of objects or more. The method does not require an existing key-management structure, such as a PKI, but provides a substrate to build such a service as part of a directory service. SDs provide a useful approach for dealing with logical keying structures for data protection in large-scale systems in which many objects must be protected.

3 Embedded biometric sensors

In literature, several approaches have been proposed to develop biometric-based recognition systems. Generally, these systems exploit filters and image enhancement algorithms, classification algorithms, and matching techniques are developed with standard high-level programming languages on general purpose computers. Unlike the software approaches, the hardware approaches allow the developers to design secure embedded biometric recognition sensors (Militello *et al.*, 2011).

The embedded solution allows for resolving security problems in biological characteristics management (*Replay Attacks*), while the use of the AES, encrypted templates transmission makes unuseful data, avoid to transmit plain-text information, making unusable the biometrics greatness intercepted (*Communication Attacks*). Finally, smartcards allow developing authentication systems with protected user credentials and no centralized databases (*Database Attacks*).

In our approaches, biometric templates are added to user (username; password) pair in order to generate secure user credentials. This solution has the advantage that data and resources access in large-scale systems is only permitted to the biological owner of the smartcard.

Computational-intensive processing tasks are often confined for real-time execution on large size workstations or expensively custom-designed hardware. The current availability of mature reconfigurable hardware, like FPGAs, coupled with the usage of development environment and hardware programming languages, offers a good path for porting such applications on embedded devices. Sensor prototyping on an FPGA is facilitated using the Handel-C algorithmic-like hardware programming language that uses a similar syntax with ANSII C with the addition of inherent parallelism.

In what follows, several developed and tested unimodal and multimodal biometric authentication systems are briefly described. Two strong and invasive biometric traits, such as fingerprint and iris, have been considered, analyzed, combined, and compared. Generally, biometric authentication systems are classified into two broad groups: micro-features and macro-features-based biometric authentication systems. Several sensors and scanners could be used for fingerprint and iris acquisition (Fingerprint Acquisition Sensor; Iris Acquisition Sensor). However, well-known databases have been used to test and evaluate the performance of the presented approaches (Chinese Academy of Sciences Institute of Automation, Fingerprint Verification Competition website, 2002; BATH Iris Database website) so that performance comparison will be possible.

3.1 Unimodal fingerprint-based architectures

The approaches proposed for developing fingerprint recognition systems can be divided into two main classes. The first class uses micro-features (minutiae) information for traits matching, while the latter class uses macro-features (core and delta singularity points) information for classification and recognition tasks. As the available optical and photoelectric sensors give high-quality fingerprint images with a well-defined core and delta points, fingerprint matching can involve two possible ways: the comparison of few features leading to fast authentication system (macro-features-based approaches) and the classical comparison of more distinctive points (micro-features-based approaches) to obtain high recognition rates and high processing time.

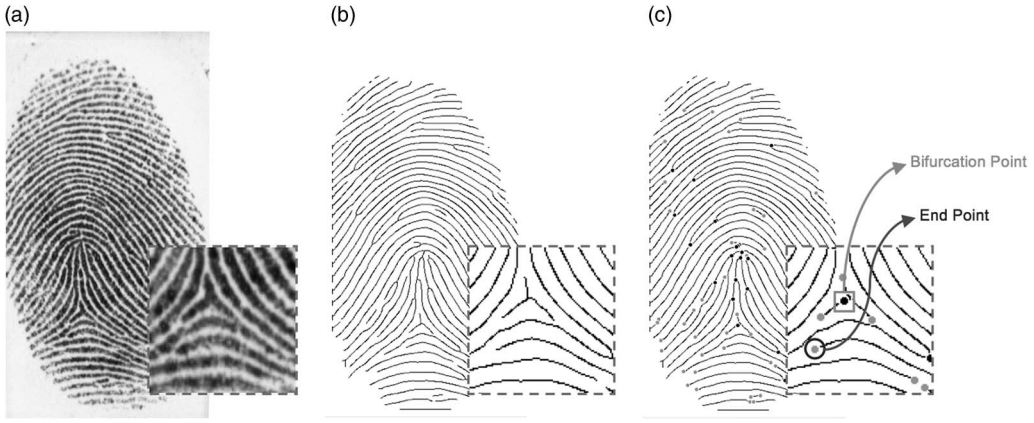

Figure 3 Fingerprint micro-features extraction steps: (a) original fingerprint image; (b) fingerprint image with thinned ridges; (c) thinned image with located minutiae

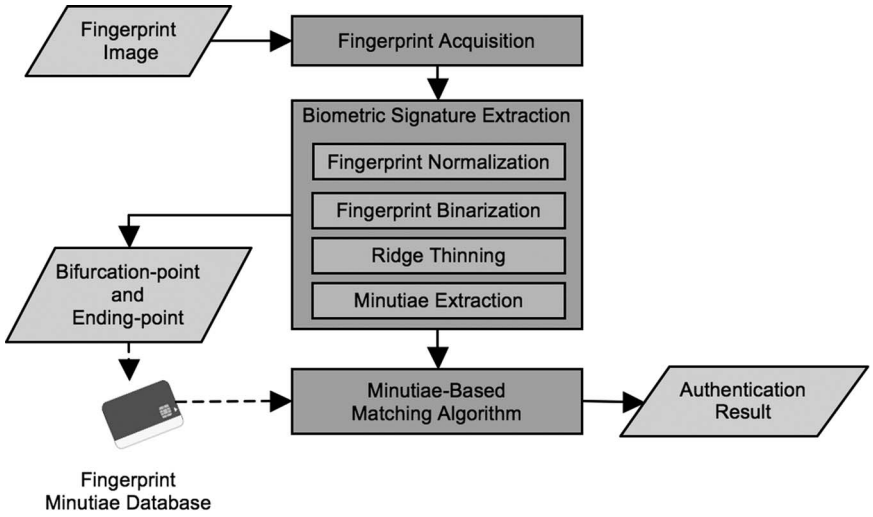

Figure 4 The flow diagram of the minutiae extraction chain in the fingerprint micro-features system

3.1.1 Spatial micro-features-based sensor (Uni-F-Micro)

In this subsection, a micro-features-based embedded biometric sensor is described (Vitabile *et al.*, 2005; Militello *et al.*, 2011). Figure 3 shows two common fingerprint micro features: bifurcations and end points.

Generally, minutiae-based authentication systems are characterized by three main steps: image acquisition, biometric signature extraction, matching between the acquired biological signature and the stored correspondent one (see Figure 4). The typical fingerprint minutiae extraction chain is composed of:

1. Normalization: generally, after the image acquisition phase, the image is overexposed or underexposed. Input image is a grayscale image with different gray levels mean and variance depending on the acquisition conditions. Several steps are performed in order to normalize it to desired mean and variance values.
2. Binarization: this operation takes as input a grayscale image and returns a binary image as output. Image intensity levels are binarized considering an adaptive local energy threshold.
3. Thinning: the thinning algorithm reduces image noise and improves the robustness of the feature extractor. This phase consists of reducing fingerprint ridge in one-bit line.
4. Minutiae extraction: it aims to extract fingerprint distinctive features (minutiae), such as endpoints and bifurcations.

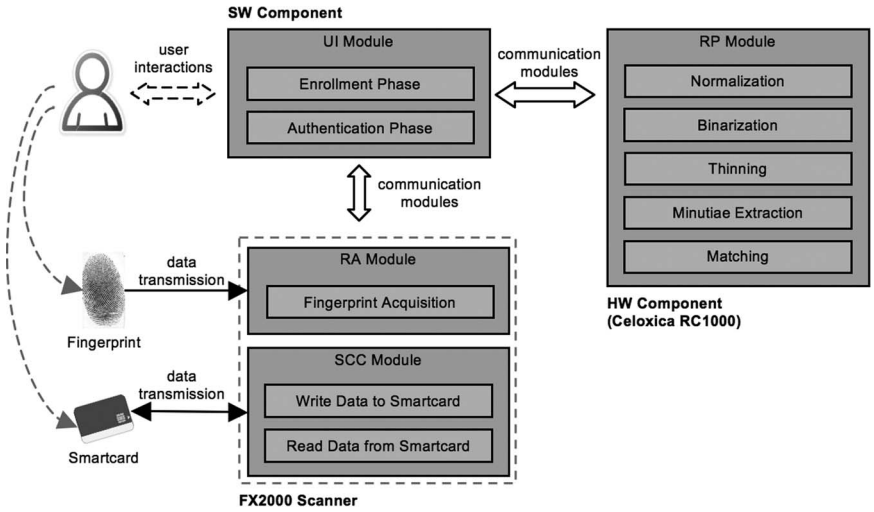

Figure 5 The four modules of the Uni-F-Micro sensor

5. Matching: it is performed using local minutiae information, such as minutiae class, its spatial coordinates, and orientation (see Figure 3).

The corresponding embedded system has been designed and prototyped using the Celoxica RC1000 board, equipped with a Xilinx Virtex-E FPGA. An FPGA-based board allows for rapid system prototyping and make possible to develop embedded authentication sensors. With more details, the embedded sensor is composed of four modules (see Figure 5):

1. The User Interface Module (UI Module) drives the access to the biometric system functionality: the enrollment phase and the authentication phase. In the first phase (the enrollment phase) the UI Module performs the procedures to acquire the user biometric feature and to store it into a smartcard, through the Recognizer Acquisition Module (RA Module). During the authentication process, the UI Module acquires the current user biometric feature and sends it to the Recognizer Processing Module (RP Module). The UI Module handles also the authentication result (authorized or denied access).
2. The RA Module deals with the fingerprint acquisition task. In this implementation, it is composed of the biometric fingerprint scanner device and the Biometric Service Provider.
3. The RP Module deals with the fingerprint processing algorithms and it is implemented on a Celoxica RC1000 board.
4. The SmartCard Communication Module is integrated into the fingerprint scanner device.

3.1.2 Spatial macro-features-based sensor (Uni-F-Macro)

The recognition system presented in this section is based on fingerprint singularity points. Generally, core and delta points are used for fingerprint classification. The delta point is the center of a triangular edge pattern, while the core point is the center of a circular edge pattern on the fingerprint image. Despite the classical approach, core and delta position, their relative distance and orientation can be used for fingerprint identification, too (Militello *et al.*, 2008). As result, the matching phase involves the comparison of few points, so that the whole system has low processing time with a reasonable accuracy.

Core and delta detections are performed by checking the Poincar indeces (Zhang *et al.*, 2004). The first step is related to directional matrix computation. Successively, using Poincar indeces obtained from directional matrix the singularity points are detected. The matching phase returns the similarity index between the processed fingerprint image and the related template. The similarity index depends on the number and the class of the extracted singularity points and its mutual positions and distances. In the last case, two weighted error distances between the core/delta pairs of the processed fingerprints and the corresponding template are considered (Militello *et al.*, 2008). With more details, to perform the

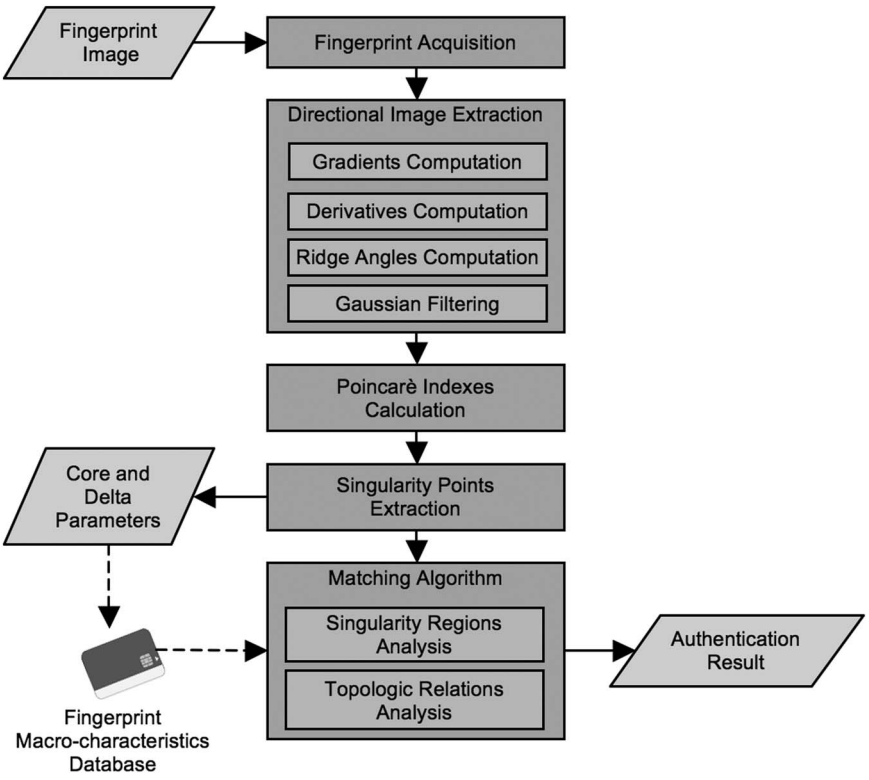

Figure 6 The flow diagram of the singularity-point extraction chain in the fingerprint macro-features system

singularity points extraction phase, two different analysis must be performed: singularity regions analysis and topological relations analysis:

1. Singularity regions analysis: the comparison between the same type of singularity points (core/core and delta/delta) is performed analyzing the directional image. The considered part of image is a round neighbor centered on the singularity point with a fixed dimension.
2. Topological relations analysis: if the two fingerprint images have at least two singularity points then the pair with smaller distance is selected. The smaller pair is chosen to decrease the distortion problem and to increase the probability to extract real singularity points.

Overall system blocks are depicted in Figure 6. The embedded sensor has been prototyped on the Celoxica RC203 board, equipped with the Xilinx Virtex-II FPGA.

3.2 Unimodal iris-based architectures

Among biometric technologies, iris recognition has received an increasing attention owing to its high reliability. Iris offers more discriminating properties and advantages with respect to other biometric technologies. As fingerprint authentication systems, iris authentication systems are characterized by three main steps: image acquisition, biometric signature extraction, and matching process between the acquired biological signature and the stored correspondent one. Different approaches have been proposed in literature to address iris-based authentication.

Unlike fingerprints, it is difficult to classify and localize apparent features in an iris image. Considering features extraction, existing iris recognition methods can be roughly divided into three major categories: the phase-based methods, the zero-crossing representation-based method, and the texture analysis-based methods. The most common approaches, also called Daugman or macro-features-based approaches, are phase-based methods using a frequency coding and integral-differential operators to process iris information (Daugman, 1993). Daugman-based approaches present several advantages, in terms of computational costs and accuracy, because of the related image transformation in the frequency domain.

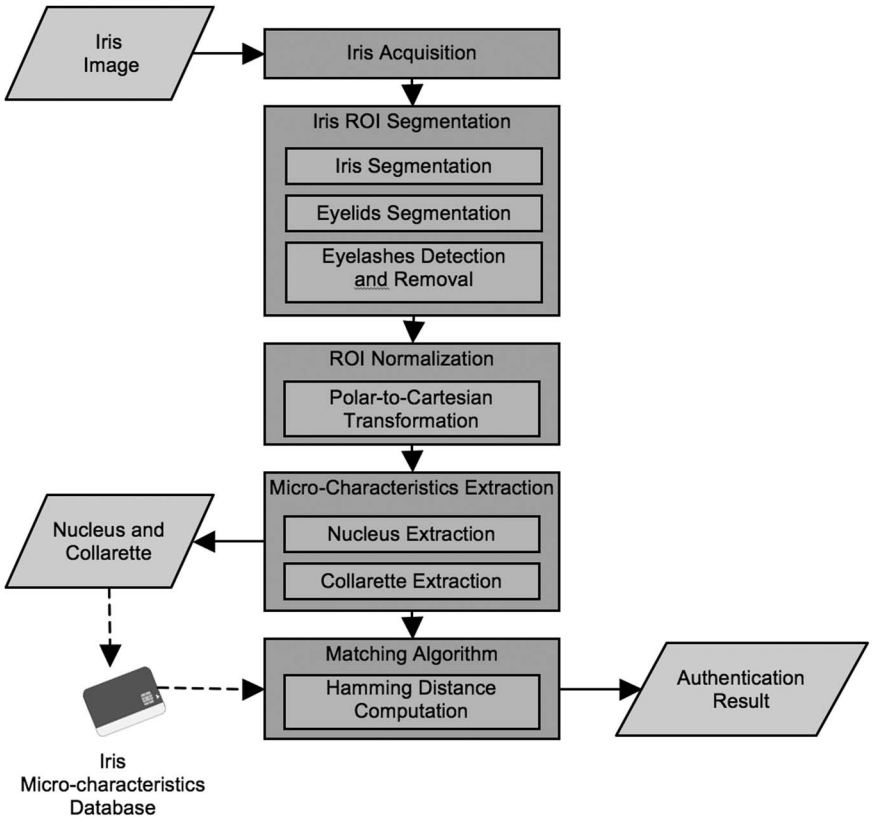

Figure 7 The flow diagram of the processing chain in the iris micro-features recognition system

However, in the last years, some researchers have identified particular useful iris micro features to develop reliable systems using the texture analysis-based methods. In De Mira and Mayer (2003), Sung *et al.* (2004), and Militello *et al.* (2010), the authors developed particular approaches based on texture analysis and iris micro features. However, these approaches require high-quality scanned images.

3.2.1 Spatial micro-features-based sensor (Uni-I-Micro)

In this section, an iris micro-features recognition sensor is described (Militello *et al.*, 2009, 2010). The approach uses the highly distinctive characteristics of iris collarette and nucleus for user authentication. The developed authentication system has been prototyped using the Celoxica RC203 board, showing good properties in terms of recognition rate, execution time, required resources, and power consumption. As depicted in Figure 7, system architecture is composed of five main blocks: iris image acquisition block, region of interest (ROI) segmentation block, ROI normalization block, micro-features extraction block, and the matching block to compare biometric descriptors. The codified iris template can be stored into a smartcard.

Dropping the image acquisition phase, the remaining processing phases are briefly described:

1. Segmentation phase: iris and pupil center and ray are first detected. Moreover, eyelids and eyelashes are also detected. Boundaries iris image are detected by means of edge detection techniques to compute the parameters of the two circles. Successively, eyelids are isolated fitting a line to the upper and lower eyelid using the linear Hough transform (Hough, 1962; Shi *et al.*, 2004). Successively, Canny edge detection algorithm (Canny, 1986) is used to create the edge map and only the horizontal gradient information is considered.
2. Normalization phase: iris of different people may be of different size. For the same person, the size may vary because of changes in illumination and other factors. In order to achieve invariance to translation, rotation, and scale, the annular iris region is normalized to a rectangular block having a fixed size.

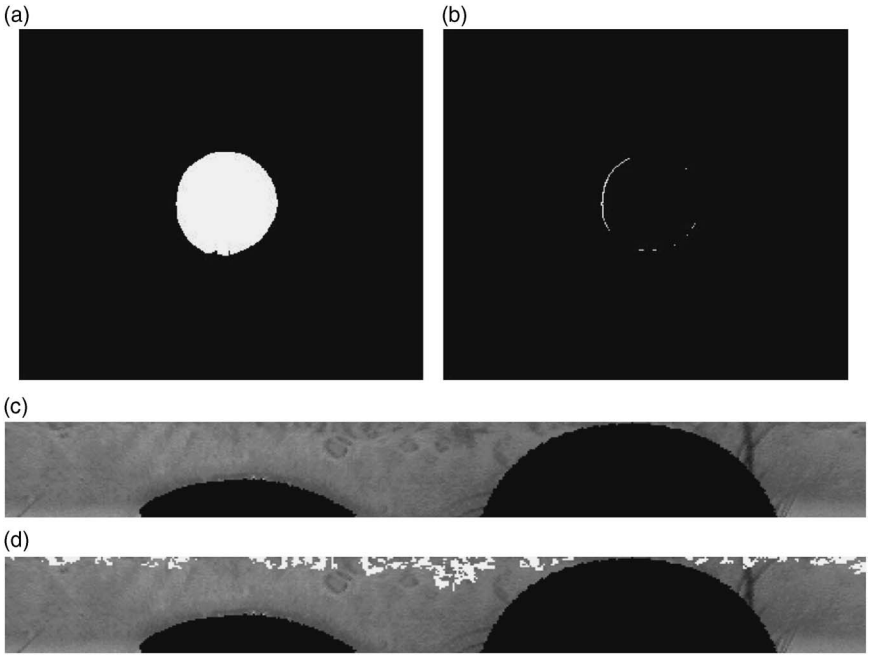

Figure 8 An example of the nucleus and collarette extraction process: (a) internal pupil zone; (b) nucleus pixels with no circular symmetry; (c) the region of interest after the segmentation and normalization phases; (d) the extracted collarette

3. Micro-features extraction phase: iris nucleus and collarette are extracted and a biometric template is built with the related information. The nucleus represents the contour of the pupil that has no circular symmetry. The collarette is confined to the inner half of the iris and contains either radial spokes or dots (the latter being either well defined or smeared).
4. Matching algorithm phase: an *ad hoc* algorithm is applied to compare the biometric template pair. The comparison of the two models of the biometric identifier corresponds to a roto-translation operation minimizing its hamming distance (HD). As shown in Equation (1), HD is defined as the sum of the discordant bits in a homologous position (XOR operations between X and Y bits):

$$HamDis = \frac{1}{N} \times \sum_{j=1}^{N} (X_j \otimes Y_j) \tag{1}$$

where N is the total number of bits.

Figure 8 shows an example of processed nucleus and collarette micro features.

3.3 Multimodal architectures

Despite their effectiveness, unimodal biometric systems have many limitations with data sensors, as captured data are often affected by noise, distinctiveness ability, that is, biometric features have not the same distinctiveness degree, and lack of universality, that is, some people do not have the biometric feature which a system might allow. Multimodal biometric systems and related fusion strategies are a recent approach developed to overcome the limits.

Fusion strategies can be divided into two main categories: pre-mapping fusion strategies (before the matching phase) and post-mapping fusion strategies (after the matching phase) (Ross & Jain, 2003). The first category deals with the feature vector fusion level: the information extracted from different sensors is stored in vectors on the basis of its modality. Feature vectors are then combined to create a joint feature vector, which is the basis of the matching and recognition process. Usually, these techniques are difficult to use because they result in many implementation problems (Ross & Jain, 2003; Conti *et al.*, 2010).

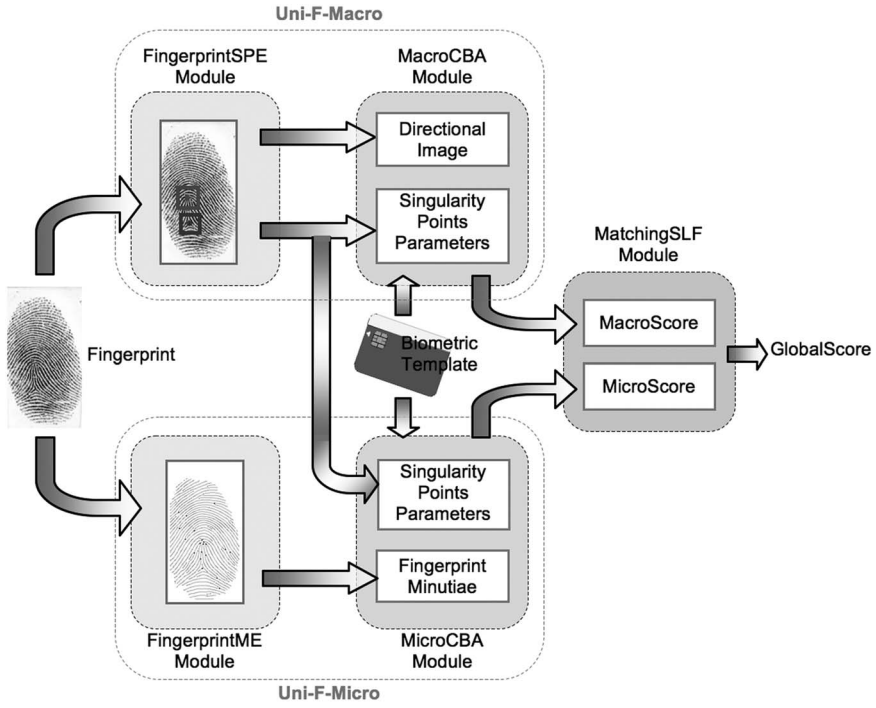

Figure 9 The block scheme of the proposed multimodal multi-algorithmic fingerprint sensor

The second category deals with the fusion at the decision level, based on some algorithms combining single decisions for each component of the system. As example, it can be used on the combination of single unimodal matching scores, after distinct feature extraction and comparison processes between stored data and test data. Starting from the matching scores or distance measures of each subsystem, an overall matching score is generated using linear or non-linear weighting. Multimodal biometric systems have demonstrated significant improvements against unimodal biometric systems, in terms of higher accuracy and high resistance to spoofing (Mane & Jadhav, 2011).

3.3.1 Spatial micro-features-based sensor (Multi-FF)

In this section, a multi-algorithmic approach to design an AFAS (automatic fingerprint authentication system) is described. The proposed architecture is composed of two AFAS modules based on micro and macro features, respectively (Conti *et al.*, 2009). Multimodal fusion is performed weighting the unimodal AFAS matching scores in order to obtain an overall matching score.

As depicted in Figure 9, an acquired fingerprint image is processed by the Fingerprint Minutiae Extraction Module (FingerprintME Module) and the Fingerprint Singularity-Points Extraction Module (FingerprintSPE Module) in order to extract useful information, such as minutiae location and orientation, core and delta location. Minutiae and singularity point information are used as inputs of the Micro-Features-Based Authentication Module (MicroCBA Module) and Macro-Features-Based Authentication Module (MacroCBA Module). The Uni-F-Micro Module, described in Section 3.1.1 and composed of FingerprintME Module and MicroCBA Module, uses singularity point information for fingerprint registration and performs fingerprint template matching using minutiae type and position (micro features). The Uni-F-Macro Module, described in Section 3.1.2 and composed of FingerprintSPE Module and MacroCBA Module, performs fingerprint template matching using only the directional image of the original fingerprint image and the information generated by the singularity points. Both modules perform fingerprint template matching after the stored template decryption, as the fingerprint templates are encrypted before their storage.

The Matching-Score-Level Fusion Module computes the overall matching score combining the two unimodal subsystem matching scores. As the Uni-F-Micro Module and the Uni-F-Macro Module are

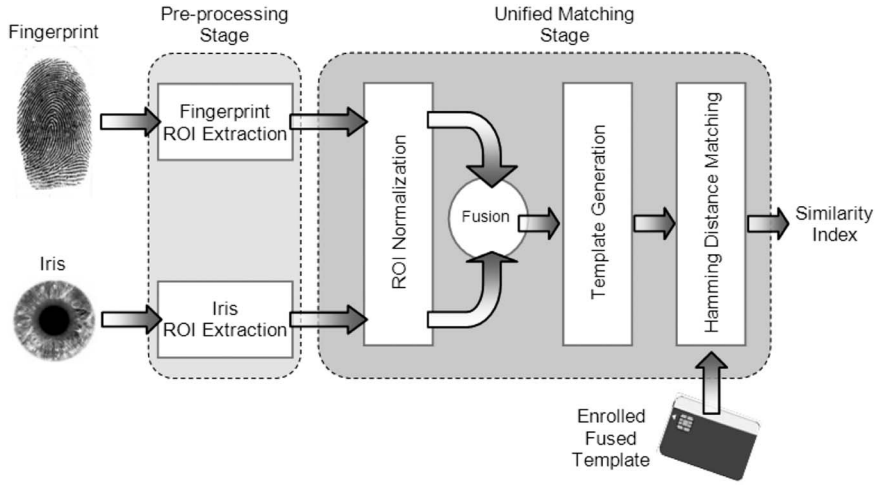

Figure 10 The general schema of the frequency-based fingerprint/iris multimodal sensor

based on different techniques and parameters, a weighted sum has been used to obtain the overall matching score. Experimental trials have demonstrated that the best performance, in terms of false acceptance rate (FAR) and false rejection rate (FRR) indeces, is obtained using Equation (2), where $K_{Mi} = 0.6$ and $K_{Ma} = 0.4$ constant values have been experimentally optimized:

$$GlobalScore = K_{Mi} \times MicroScore + K_{Ma} \times MacroScore \tag{2}$$

3.3.2 Frequency-based fingerprint/iris multimodal sensor (Multi-FI)

In this section, a template fusion technique for designing a multimodal identification system is described (Conti *et al.*, 2010). The corresponding embedded sensor is a multimodal fingerprint and iris recognizer. As shown in Figure 10, iris and fingerprint images are pre-processed to extract the ROIs surrounding some meaningful points. Extracted ROIs are processed and codified in the frequency domain, resulting in an homogenous template in which fingerprint and iris information have the same representation. The final homogenous biometric vector integrates two sub-patterns and it is composed of binary sequences representing the unified biometric template. The first pattern is related to the extracted fingerprint singularity points, reporting the codified and normalized fingerprint ROIs. The second pattern is related to the extracted iris code, reporting the codified and normalized iris ROIs. Normalized fingerprint and iris ROIs are then codified using the Log-Gabor approach (Field, 1987) in the frequency domain. The matching algorithm based on the HD (see Equation (1)) is able to work on the unified and homogenous template in order to give the appropriate similarity degree. If two patterns are completely independent, it will be HD = 0.5, while two patterns of the same biometric descriptor have HD = 0. A tamper-resistant smartcard can be used for template memorization.

3.4 Traits and approaches analysis

Fingerprint authentication systems can exploit many distinctive points (minutiae) or few distinctive points (core and delta). Minutiae-based systems need a complex pre-processing phase to reduce noise and false minutiae and, consequently, high processing time. On the other hand, minutiae are in great number in fingerprint (or portion of it), so that a fingerprint matcher has many information to compare a fingerprint pair. Singular points-based systems need a light pre-processing phase aimed to select core and delta points. Authentication systems are faster than the previous ones, but its accuracy is low when singular point segmentation fails. However, in both cases, fingerprint image quality has a strong, definitive impact on systems accuracy and performance.

Iris-based recognition systems can use iris macro features in frequency domain or iris micro features in spatial domain. The first class considers the whole iris portion leading to fast processing time and high accuracy systems (Daugman, 1993). Image quality has a limited impact on them, so that medium/high

Table 1 Sensor prototyping general information

Sensor	Trait	Processing approach	FPGA board
Uni-F-Macro	Fingerprint	Spatial macro features	RC203E
Uni-F-Micro	Fingerprint	Spatial micro features	RC1000
Uni-I-Micro	Iris	Spatial micro features	RC203E
Multi-FF	Fingerprint	Spatial macro features	RC203E
	Fingerprint	Spatial macro features	RC1000
Multi-FI	Fingerprint	Frequency macro features	RC203E
	Iris	Frequency macro features	RC203E

FPGA, field-programmable gate arrays.

image quality leads to very interesting systems. Micro-features or texture-based authentication systems are based on iris micro information extraction and matching. The procedure requires high-quality images and high processing time. However, increasing scanner quality can produce interesting systems in the near future.

Multimodal authentication systems use two or more biometric traits for user authentication. System accuracy increases reducing both false acceptance and false rejection events. Multimodal systems require complex hardware structure if compared with the single unimodal composing systems. They usually require high computational resources and high processing time. Template-level fusion methods produce higher accuracy systems, even if the majority of work published on this topic had been based on matching-score-level fusion or decision-level fusion (Conti *et al.*, 2010)).

4 Experimental results

This section presents the experimental results achieved by the unimodal and multimodal hardware biometric sensors, in terms of hardware resources analysis, time-execution analysis, and recognition performance analysis. A further analysis with comparable literature works is reported as well.

4.1 Software and hardware environment

Handel-C language (Mentor Graphics website), DK Design Suite (Mentor Graphics website), and Xilinx ISE (Xilinx website) software development tools have been used for sensor prototyping. Handel-C is an algorithmic-like hardware programming language that uses a similar syntax with ANSII C with the addition of inherent parallelism. Table 1 shows the sensors prototyping information (traits, processing approach, FPGA board used, Mentor Graphics website), while Figure 11 shows FPGA physical resources used for the design implementation of the described sensors.

4.2 Time-execution analysis

Biometric sensors rapid prototyping on FPGA leads to highly competitive systems in terms of execution time and speed-up factors. Table 2 shows the needed execution time to complete the whole authentication task. To evaluate the effectiveness of the presented hardware implementations, it is interesting to compare the FPGA-based implementation with the corresponding software one. Considering a Pentium 4 general purpose processor clocked at 2.4 GHz, the correspondent potential speed-up factors are depicted in the same table.

The low working frequency suggests interesting considerations for the employment of the embedded sensors in portable devices, as 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 (Militello *et al.*, 2010).

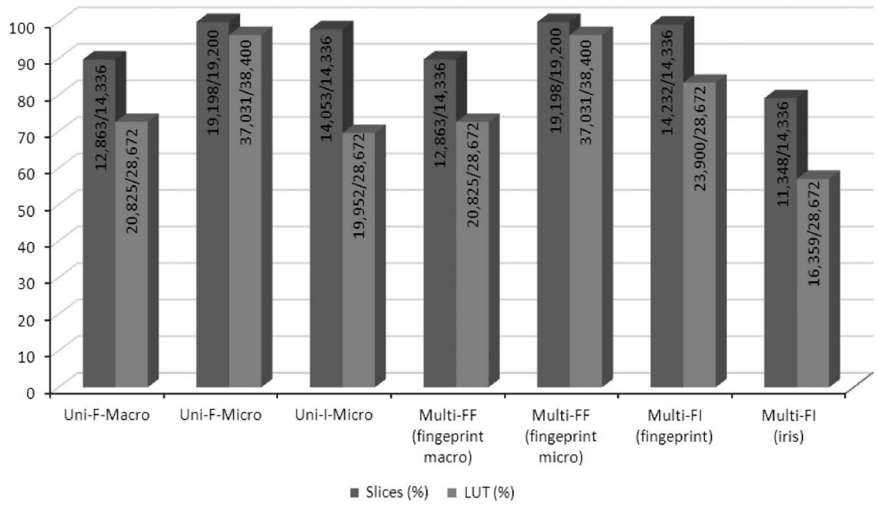

Figure 11 Used/available slices and look-up tables needed for sensor prototyping. Multimodal systems use two parallel field-programmable gate arrays boards

Table 2 Processing cycles, processing times, working frequencies, and speed-up factors of the prototyped sensors

Sensor	Working frequency (MHz)	Cycle number	Execution time (ms)	Speed-up factor
Uni-F-Macro	25.175	875×10^3	34.8	3×
Uni-F-Micro	22.5	$11\,565 \times 10^3$	514.1	8×
Uni-I-Micro	25.175	$12\,143.1 \times 10^3$	482.3	10×
Multi-FF	25.175	875×10^3	34.8	3×
	22.5	$11\,565 \times 10^3$	514.1	3×
Multi-FI	25.175	$17\,140 \times 10^3$	680.82	7×
	25.175	$14\,767 \times 10^3$	586.57	7×

Speed-up factors are computed against the corresponding software implementation on 2.4 GHz general purpose processor.

4.3 Recognition performance analysis

Sensor recognition rate has been evaluated using the well-known FRR and FAR indeces. The FAR is the number of times that an incorrectly accepted unauthorized access occurs, while the FRR is the number of times that an incorrectly rejected authorized access results. Figure 12 shows the achieved recognition rates, in terms of FAR and FRR, of the different implementations and processing approaches.

5 Discussions and comparisons

A trusted biometric authentication system has to reduce the point-of-attacks in the recognition chain (Ambalakat, 2005). The proposed approach aims to integrate passive scanners and processing boards to prototype-embedded biometric sensors. Old fingerprint scanners could be attacked using fake, gummy, and artificial fingers (Matsumoto *et al.*, 2002). However, several recent technologies, including temperature sensors, IR sensors, and pulse checking sensors, are available to employ secure scanners in trusted biometric authentication systems. Several works on biometric recognizer hardware implementation have been proposed.

In Bonato *et al.* (2003), the authors proposed a hardware system using a pipeline technique to increase the final output. The needed fingerprint pre-processing tasks had been implemented on the Altera FLEX10KE FPGA. Initially, a Gaussian filtering is used to enhance fingerprint quality and an edge-detection algorithm is applied to segment fingerprint ridges. Finally, a thinning algorithm is applied before minutiae

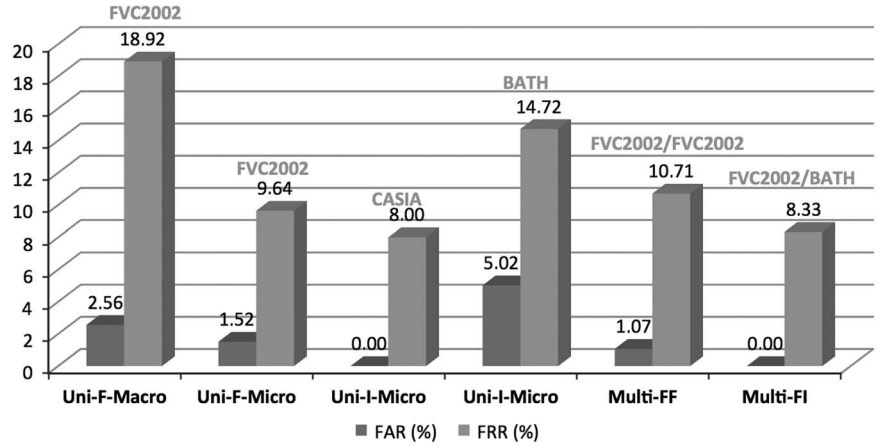

Figure 12 Recognition rates achieved by the proposed sensors. The figure also shows the used databases

localization. The processing time takes 306.93 ms. However, fingerprint matching time was not reported by the authors.

In Schaumont *et al.* (2003), the authors developed an embedded device for fingerprint matching operations. ThumbPod uses multiple levels of programming (Java, C, and hardware) with a hierarchy of programmable architectures (KVM on top of an SPARC core on top of an FPGA). The bottom system layer is composed of a Xilinx Virtex-II XC2V1000 FPGA, on which the authors configured a soft-core processor with two hardware coprocessors. In addition, an encryption processor and a Discrete Fourier Transform signal processor provide acceleration for the computational critical components. The authors evaluated its implementation by means of FAR (0.01%) and FRR (0.5%) indeces. However, no description and details of the used databases are reported in the paper. Average execution time is in the range 4–6 seconds.

In Miyazawa *et al.* (2006), the authors presented a DSP prototype implementation of a previously proposed phase-based matching algorithm for iris recognition. The authors implemented a compact version of their method on the hardware device and evaluated their approach using the CASIA database. Authors reported either the ROC (receiver operating characteristic) curve or the EER (equal error rate) index. Analyzing their results, the system shows the following indeces: EER = 8.3%, FMR (false match rate) = 0%, FNMR (false non-match rate) = 25%. The overall iris recognition procedure takes 1 second on the DSP device (Texas Instruments TMS320DM641, 400 MHz).

In Yoo *et al.* (2007), the design of embedded multimodal biometric systems is analyzed. The authors have implemented a real-time system using an hardware platform composed of a low power ARM920T S3C2440A (400 MHz) core processor and a connected Xilinx XC3S4000 FPGA. Initially, the system was implemented on the ARM processor and then the most time-consuming biometric system components were implemented on FPGA. They used the ETRI face database, the CASIA V.1.0 iris image database (Chinese Academy of Sciences Institute of Automation), and the FVC 2004 DB3 fingerprint database to test the performance of each single unimodal biometric system by means of the EER index. The presented results show EER = 1.50% for the face-based identification system, EER = 1.68% for the iris-based identification system, and EER = 4.53% for the fingerprint-based identification system. Execution times are 1.2, 1.0, and 1.8 seconds, respectively. No fusion techniques and results were presented for the multimodal system.

In Lopez and Canto (2008), a minutiae extraction algorithm implemented on a Xilinx Spartan 3 FPGA is proposed. The embedded coprocessor processes a 256 × 256 fingerprint image in 262 ms. In Fons *et al.* (2006), a work focused on the implementation of a physical fingerprint matcher implemented on FPGAs is proposed. Several application-specific coprocessors were synthesized in order to speed up the overall minutiae-based application. The system was implemented on the Atmel AT40K FPGA showing a 25–40 ms enrollment time and a 7.2 ms matching time. In Garcia and Canto Navarro (2006), a dedicated coprocessor specialized on the development of a fingerprint ridge extraction algorithm is proposed. The coprocessor was synthesized on a Xilinx FPGA Spartan 3. As a result, the coprocessor processes a 256 × 256 fingerprint image in 262 ms.

Table 3 Embedded recognizer processing times and working frequencies

Sensor	Trait	Hardware platform	Working frequency (MHz)	Processing time (ms)
Bonato *et al.* (2003)	Fingerprint	Altera FLEX10KE	NA	306.93
Schaumont *et al.* (2003)	Fingerprint	Xilinx Virtex-II XC2V1000	NA	4000–6000
Miyazawa *et al.* (2006)	Iris	TI TMS320DM641 DSP	400	1000
Yoo *et al.* (2007)	Iris	ARM 920TS3C2440A	400	1000
Lopez and Canto (2008)	Fingerprint	Xilinx Spartan 3	40	262
Fons *et al.* (2006)	Fingerprint	Atmel AT40K	25	32.2–47.2
Garcia and Canto Navarro (2006)	Fingerprint	Xilinx Spartan 3	52	262
Vitabile *et al.* (2005)	Fingerprint	Xilinx Virtex-E	22.5	541
Militello *et al.* (2008)	Fingerprint	Xilinx Virtex-II	25.175	34.8
Militello *et al.* (2010)	Iris	Xilinx Virtex-II	25.175	482.3
Conti *et al.* (2010)	Fingerprint/ iris	Xilinx Virtex-II	25.175	680.2

In Bonato *et al.* (2003), the matching time is not included.

Table 4 Databases and recognition indeces comparison

Sensor	Type	Trait	Database	FAR (%)	FRR (%)	ERR (%)
Bonato *et al.* (2003)	Unimodal	Fingerprint	Proprietary	NA	NA	NA
Schaumont *et al.* (2003)	Unimodal	Fingerprint	Proprietary	0.01	0.50	NA
Miyazawa *et al.* (2006)	Unimodal	Iris	CASIA	0.00	25.00	8.30
Yoo *et al.* (2007)	Unimodal	Face Iris Fingerprint	ETRI CASIA FVC2004	NA	NA	1.50 1.68 4.53
Uni-F-Macro	Unimodal	Fingerprint	FVC2002	2.56	18.92	NA
Uni-F-Micro	Unimodal	Fingerprint	FVC2002	1.52	9.64	NA
Uni-I-Micro	Unimodal	Iris	BATH	5.02	14.72	NA
Uni-I-Micro	Unimodal	Iris	CASIA	0	8	NA
Multi-FF	Multimodal	Fingerprint	FVC2002	1.07	10.71	NA
Multi-FI	Multimodal	Fingerprint/iris	FVC2002/BATH	0.00	8.33	4.46

FAR, false acceptance rate; FRR, false rejection rate; ERR, equal error rate.

In Table 3 the processing times and the used hardware platforms for prototyping-embedded unimodal sensors are depicted. Even if a direct comparison is difficult to obtain, as the prototyping platforms and the used database are different, the macro-feature-based system shows interesting performance in terms of processing time (80% reduction, considering the different working frequencies). The multimodal system gives higher processing time, but very interesting recognition rates (Conti *et al.*, 2010). In Table 4 the recognition rates for the different literature approaches are reported. Unimodal systems have comparable performance considering the current literature approaches. Multimodal systems show better recognition rates when compared against the corresponding single unimodal system. However, the hardware structures needed for its implementations considerably grow.

6 Conclusions

Embedded biometric sensors overcome the security limits of conventional software recognition systems, hiding its common attack points. Biometric traits processing and matching are performed into the embedded sensor without biometric data transmission before user authentication. The use of tamper-resistant smartcards

provide a secure environment to store biometric templates. In addition, no distributed or centralized databases are needed, avoiding the presence of critical point of failures. Prototyped-embedded biometric sensors show interesting results in terms of recognition rates, processing time, and speed-up factors. Sensor recognition rate has been evaluated using the well-known FRR and FAR indeces against the common well-known fingerprint and iris databases. Processing cycles number have been considered to compare embedded sensor performance and the corresponding software implementation, running on a general purpose processor. Embedded multimodal sensors show interesting FAR and FRR working points, comparable processing time, limited hardware resources and they are particularly suitable for secure applications.

References

Agrawal, D., Archambeault, B., Rao, J. & Rohtagi, P. 2003. The em-side channel(s). In *Workshop on Cryptographic Hardware and Embedded Systems, CHES*. LNCS, **2523**, 29–45. Springer.

Ambalakat, P. 2005. *Security of Biometric Authentication Systems, 21st Computer Science Seminar*, SA1-T1-1, 2, www.rh.edu/rhb/csseminar2005/SessionA1/ambalakat.pdf.

BATH Iris Database website, 2004. http://www.smartsensors.co.uk/irisweb/ (accessed 21 November 2014).

Bonato, L. V., Molz, R. F., Furtado, J. C., Ferrão, M. F. & Moraes, F. G. 2003. (a) Design of a fingerprint system using a hardware/software environment. In *Proceedings of the 2003 ACM/SIGDA 11th International Symposium on Field Programmable Gate Arrays*, v.1, 240–240, ACM New York press. ISBN: 1-58113-651-X.

Canny, J. 1986. A computational approach to edge detection. *IEEE Transactions on Pattern Analysis and Machine Intelligence* **8**, 679–698.

Chinese Academy of Sciences Institute of Automation (CASIA) Iris Image Database (ver. 1.0) 2002. http://www.nlpr.ia.ac.cn/english/irds/Databases/databases.html (accessed 21 November 2014).

Conti, V., Militello, C., Sorbello, F. & Vitabile, S. 2010. 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* **40**(4), 384–395.

Conti, V., Militello, C., Vitabile, S. & Sorbello, F. 2009. A multimodal technique for an embedded fingerprint recognizer in mobile payment systems. *International Journal of Mobile Information Systems* **5**(2), 105–124.

Daugman, J. G. 1993. High confidence visual recognition of persons by a test of statistical independence. *IEEE Transactions on Pattern Analysis and Machine Intelligence* **15**(11), 1148–1161.

De Mira, J. Jr. & Mayer, J. 2003. Image feature extraction for application of biometric identification of iris – a morphological approach. In *Proceedings of the XVI Brazilian Symposium on Computer Graphics and Image Processing*, **1**, 12–20.

Field, D. J. 1987. Relations between the statistics of natural images and the response profiles of cortical cells. *Journal of the Optical Society of America*, **4**, 2379–2394.

Fingerprint Acquisition Sensor website, 2002. http://www.biometrika.it/eng/fx2000.html (accessed 21 November 2014).

Fingerprint Verification Competition website 2002. http://bias.csr.unibo.it/fvc2002/ (accessed 21 November 2014).

Fons, M., Fons, F. & Canto, E. 2006. Design of FPGA-based hardware accelerators for on-line fingerprint matcher systems. *Research in Microelectronics and Electronics*, 333–336, doi: 10.1109/RME.2006.1689964.

Garcia, M. L. & Canto Navarro, E. F. 2006. FPGA implementation of a ridge extraction fingerprint algorithm based on microblaze and hardware coprocessor. In *International IEEE Conference on Field Programmable Logic and Applications*, ISBN 1-4244-0312-X, 1–5.

Hough, P. V. C. 1962. Method and Means for Recognizing Complex Patterns. US Patent 3.069.654.

Iris Acquisition Sensor, 2010. http://uidai.gov.in/biometric-devices.html (accessed 21 November 2014).

Kocher, P. C. 1999. *Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and Other Systems*, Cryptography Research Inc. http://cryptography.com.

Kocher, P. C., Jaffe, J. & Benjamin Jun, B. 1999. *Differential Power Analysis*, Cryptography Research Inc. http://cryptography.com.

Lopez, M. & Canto, E. 2008. FPGA implementation of a minutiae extraction fingerprint algorithm. In *IEEE International Symposium on Industrial Electronics*, 1920–1925.

Mali, M., Novak, F. & Biasizzo, A. 2005. Hardware implementation of AES algorithm. *Journal of Electrical Engineering* **56**(9–10), 265–269.

Mane, V. M. & Jadhav, D. V. 2011. Review of multimodal biometrics: applications, challenges and research areas. *International Journal of Biometrics and Bioinformatics (IJBB)* **3**(5), 90–95.

Matsumoto, T., Matsumoto, H., Yamada, K. & Hoshino, S. 2002. Impact of artificial gummy fingers on fingerprint systems. In *Proceedings of the SPIE*, van Renesse, R. L. (ed.), Optical Security and Counterfeit Deterrence Techniques IV **4677**, 275–289.

Mentor Graphics website 2008. `http://www.mentor.com/products/fpga/handel-c/dk-design-suite/`, `http://www.mentor.com/products/fpga/handel-c/rc-series-platforms/` (accessed 21 November 2014).

Michener, J. R. & Acar, T. 2000. Security domains: key management in large-scale systems. *IEEE Software* **17**(5), 52–58.

Militello, C., Conti, V., Vitabile, S. & Sorbello, F. 2008. A novel embedded fingerprints authentication system based on singularity points. In *Proceedings of the 2nd International Conference on Complex, Intelligent and Software Intensive Systems*, ISBN/ISSN: 0-7695-3509-1. IEEE Computer Society, 72–78.

Militello, C., Conti, V., Vitabile, S. & Sorbello, F. 2009. An embedded module for iris micro-characteristics extraction. In *Proceedings of the 3rd International Conference on Complex, Intelligent and Software Intensive Systems*. IEEE Computer Society Press, 223–230.

Militello, C., Conti, V., Vitabile, S. & Sorbello, F. 2010. An embedded iris recognizer for portable and mobile devices. *International Journal of Computer Systems Science and Engineering (IJ-CSSE)* **25**(2). Special Issue on Frontiers in Complex, Intelligent and Software Intensive Systems. 119–131.

Militello, C., Conti, V., Vitabile, S. & Sorbello, F. 2011. Embedded access points for trusted data and resources access in HPC systems. *The Journal of Supercomputing* **55** (1) Special Issue on High Performance Trusted Computing. 4–27.

Miyazawa, K., Ito, K., Aok, T., Kobayashi, K. & Katsumata, A. 2006. An iris recognition system using phase-based image matching, In *IEEE International Conference on Image Processing*, 325–328.

Nielsen, R. & Hamilton, B. A. 2005. Observations from the deployment of a large scale PKI. In *4th Annual PKI R&D Workshop: Multiple Paths to Trust*. NIST, April 19–21.

Niu, Z., Zhou, K., Jiang, H., Yang, T. & Yan, W. 2009. Identification and authentication in large-scale storage systems. In *IEEE International Conference on Networking, Architecture, and Storage*, 421–427.

Oey, M. A., Warnier, M., Brazier, F. M. T. 2010. Security in large-scale open distributed multi-agent systems. In *Autonomous Agents*, ISBN 978-953-307-089-6, Kordic, V. (ed.). InTech, 107–129. `http://www.intechopen.com/articles/show/title/security-in-large-scale-open-distributed-multi-agent-systems`.

Ross, A. & Jain, A. 2003. Information fusion in biometrics. *Pattern Recognition Letters* **24**, 2115–2125.

Schaumont, P., Sakiyama, K., Fan, Y., Hwang, D., Yang, S., Hodjat, A., Lai, B. & Verbauwhede, I. 2003. Testing ThumbPod: softcore bugs are hard to find. In *8th IEEE International High-Level Design Validation and Test Workshop*, ISBN:0-7803-8236-6, 77–82.

Shi, J. Q. Z., Zhao, X. & Wang, Y. 2004. A novel fingerprint matching method based on the Hough transform without quantization of the Hough space. In *Proceedings of the 3rd International Conference on Image and Graphics*, ISBN: 0-7695-2244-0, 262–265.

Snijder, M. 2006. *Security & Privacy in Large Scale Biometric Systems*, EC JRC/IPTS, European Biometrics Forum, September 25.

Sung, H., Lim, J., Park, J. & Lee, Y. 2004. Iris recognition using collarette boundary localization. In *Proceedings of the 17th International IEEE Conference on Pattern Recognition*, **4**, 857–860.

UK Biometrics Working Group (BWG) 2003. *Biometrics Security Concerns*. BWG.

Vitabile, S., Conti, V., Lentini, G. & Sorbello, F. 2005. An intelligent sensor for fingerprint recognition. In *Proceedings of the International Conference on Embedded and Ubiquitous Computing*, ISBN: 3-540-30807-5, Lecture Note in Computer Science **3824**, 27–36. Springer-Verlag.

Xilinx website 2008. `http://www.xilinx.com/` (accessed 21 November 2014).

Yoo, J. H., Ko, J. G., Chung, Y. S., Jung, S. U., Kim, K. H., Moon, K. Y. & Chung, K. 2007. *Design of Embedded Multimodal Biometric Systems*, 3rd International IEEE Conference on Signal-Image Technologies and Internet-Based System, pp. 1058-1062, DOI 10.1109/SITIS.2007.130.

Zhang, H., Yin, Y. & Ren, G. 2004. An improved method for singularity detection of fingerprint images. *Book Advances in Biometric Person Authentication*. Publisher Springer Berlin/Heidelberg. **3338**, 516–524. ISBN 978-3-540-24029-7.