Mobile Information Systems 5 (2009) 105–124
DOI 10.3233/MIS-2009-0076
IOS Press

A multimodal technique for an embedded fingerprint recognizer in mobile payment systems

V. Conti[a], C. Militello[a], F. Sorbello[a] and S. Vitabile[b]
[a]*Dipartimento di Ingegneria Informatica, University of Palermo, Viale delle Scienze, Ed. 6 – 90128 - Palermo, Italy*
E-mails: {conti, militello, sorbello}@unipa.it
[b]*Dipartimento di Biotecnologie Mediche e Medicina Legale, University of Palermo, Via del Vespro, 129 – 90127 - Palermo, Italy*
E-mail: vitabile@unipa.it

Abstract. The development and the diffusion of distributed systems, directly connected to recent communication technologies, move people towards the era of mobile and ubiquitous systems. Distributed systems make merchant-customer relationships closer and more flexible, using reliable e-commerce technologies. These systems and environments need many distributed access points, for the creation and management of secure identities and for the secure recognition of users. Traditionally, these access points can be made possible by a software system with a main central server. This work proposes the study and implementation of a multimodal technique, based on biometric information, for identity management and personal ubiquitous authentication. The multimodal technique uses both fingerprint micro features (minutiae) and fingerprint macro features (singularity points) for robust user authentication. To strengthen the security level of electronic payment systems, an embedded hardware prototype has been also created: acting as self-contained sensors, it performs the entire authentication process on the same device, so that all critical information (e.g. biometric data, account transactions and cryptographic keys), are managed and stored inside the sensor, without any data transmission. The sensor has been prototyped using the Celoxica RC203E board, achieving fast execution time, low working frequency, and good recognition performance.

Keywords: Ubiquitous authentication, multimodal systems, mobile payment systems, biometric techniques, and embedded systems

1. Introduction

Today ubiquitous computer networks and distributed applications are changing the way people communicate with each other, creating a revolution by providing a lot of services and functionalities, requiring distributed access mechanisms rather than a single access point [11].

Mobile commerce, one of the most important distributed and mobile applications, involves both business and public administration issues. It changes the way in which people live and interact with each other. Mobile system security is one of the main issues to be considered in all payment processes [14]. These systems must provide secure access services: this is a serious problem because mobile and ubiquitous computing applications typically involve interactions between a large number of entities (e.g. people, server, etc.) across different organizations. Uncontrolled disclosure of information or unconstrained interaction of these entities could cause extremely severe consequences. Information exchange, between different systems or sub-systems, needs to be done through secure channels to ensure data confidentiality and integrity, in order to protect the available services from unauthorized use. The requirement of trusted access-points involves an high computational load for the application, because it must provide additional functionalities for users authentication, credentials verification, and secure communication strategies, starting from each system's access-point [12,13].

Biometric authentication systems, using physiological characteristics for the authentication of its users, have become most popular, mainly for their high capabilities of user discrimination (selectivity) to prevent fraud. Generally, these systems are based on three principal steps:

a) fingerprint image acquisition;
b) digital biometric signature extraction;
c) matching, i.e. the comparison between the acquired biometric signature and one or more stored signatures.

A fingerprint can be used for personal identification because of its uniqueness and invariability of the pattern of ridges and valleys in a fingertip. The immutability of the features renders fingerprint-based authentication systems extremely strong and robust. At the same time, however, biometry is a severe weakness: if biometric data is stolen, it will be permanently compromised and unlike IDs, passwords, and certificates it cannot be replaced. Typical strategies implemented in Identity Management Systems could be useful to protect biometric information.

In this paper a multimodal biometric system, combining two fingerprint authentication sub-systems is proposed. Using the proposed approach, some biometric unimodal authentication system limitations have been reduced. The proposed multimodal biometric system is composed of two main modules: the *Micro-Characteristics-Based Authentication Module* (*MicroCBA Module*) and the *Macro-Characteristics-Based Authentication Module* (*MacroCBA Module*). In addition, an embedded fingerprint recognizer has been prototyped, using the Celoxica RC203E board [26], as main component of a mobile payment system. The objective of the hardware recognizer is to overcome some of the limits of the conventional software fingerprint recognition systems, such as the vulnerability to attack related to the biometric data transmission and management. The proposed recognizer can be considered as a self-contained biometric sensor, designed to provide a device for secure authentication in mobile payment transactions. With this approach, fraud and authorization risks on mobile devices can be greatly reduced [24,25].

Typical goodness indexes have been used to evaluate the performance of the proposed system. The FAR (False Acceptance Rate) and FRR (False Rejection Rate) indexes depend on the percentage of the considered minutiae in the matching phase. An interesting trade-off of the multimodal software system is reached with FAR = 1.07% and FRR = 10.71% for the FVC2002/DB2 database [31]. In addition, the embedded hardware prototype has achieved interesting results, in terms of execution time (34.84 ms), working frequency (25.175 MHz), and FAR- FRR indexes (1.89%–11.43%) on a proprietary database captured through the Biometrika FX2000 [30] optical scanner.

The paper is organized as follows: Section 2 illustrates the features of the biometric mobile payment systems and the general issues regarding biometric identity management. Section 3 describes the standard techniques for fingerprint recognition. Section 4 describes the standard multimodal biometric systems. Section 5 describes the proposed multimodal technique as well as the achieved recognition results. Section 6 illustrates the prototyped self-contained fingerprint recognizer as well as the achieved results. Finally, section 7 reports the conclusion of this work.

2. Biometric mobile payment systems

Recent technology advances enable portable computers and electronic devices to be equipped with wireless interfaces, allowing networked communication even while these pieces of equipment are in motion. These devices offer a new paradigm of computing, in which, users are able to access shared information on portable devices, through the available infrastructure, independent of their geographical location. Mobile system communications need preconditions for authenticity and credentials validity of both sides (i.e. user and application) to establish a reliable session based on trusted information transmission, privacy, and security. Thus, users receive required services according to their identities and trust level.

Traditional authentication methodologies are based on what the user knows (passwords and userIDs) or on what the user has (badges, smartcards). However, the above security countermeasures could not be sufficient for those applications, such as mobile payment services, requiring high security levels in the authentication process. Different fatal limitations can be found in the conventional methodologies, such as easiness to forget, lose, leak and intercept the userIDs, passwords, or smartcards. The most secure and effective method for individual authentication involves the verification of unique and personal biometric features.

Locally or remote authentication methods are necessary since people must be able to access services and information everywhere. For example, the design of mobile payment systems has added another layer of complexity through the use of constrained devices with different capabilities and network limitations. Mobile payments, when executed via a mobile network, must be subject to the same level of standardization that governs physical payment card use in order to be perceived as familiar and secure. So, a secure authentication infrastructure is necessary in mobile and ubiquitous systems. A ubiquitous authentication system should be able to reduce the point-of-attacks of conventional authentication systems and supply the truly capability to authenticate people, across applications and networks. In reference to the vulnerability, a mobile biometric identification system is able to scan and map the biometric characteristics for users, register them on a database, creating a template that can be checked against all further scans to verify the user's identity. A biometric system can be considered trusted if and only if it withstands some typical attacks [15]:

- *Replay Attacks:* attacks due to the replication of information processed during the authentication process;
- *Communication Attacks:* attacks valued in terms of resistance to the interceptions of the information during its transmission;
- *Database Attacks:* attacks due the manipulation of information contained in the database.

A possible solution is the implementation of an embedded sensor, containing encrypted biometric templates, implementing the whole processing module with no biometric data transmission before user authentication. In addition, the choice of an embedded device overcomes some limits such as system performance and response time, in addition to more specific problems such as vulnerability and accessibility to personal information.

2.1. A self-contained recognizer for mobile payment systems

As reported in the previous section, a biometric system can be considered trustworthy only if it withstands some typical attacks [15]: *Replay Attacks*, *Communication Attacks* and *Database Attacks*. In this work, an embedded self-contained fingerprint recognizer has been prototyped on a FPGA-based board (Field Programmable Gate Array) [26]. The prototyped recognizer overcomes safety problems in the treatment of the biometric features (Replay Attacks) using the Advanced Encryption Standard (AES) to encrypt/decrypt biometric signatures stored in FPGA memory. The use of the AES algorithm also overcomes the problem of unauthorized access to the stored biometric templates (Database Attacks). With this approach, 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 user authentication is made. In addition, the choice of a FPGA-based device enhances the designed sensor performance in terms of both execution time and working frequency. The self-contained sensor has been prototyped using the Biometrika FX2000 fingerprint scanner [30], as the acquisition module, and the Celoxica RC203E board [26], equipped with a Xilinx VirtexII FPGA [28], as the fingerprint processing engine.

2.2. Biometric identity management

Identity management in an electronic environment involves registration, storage, protection, issuance and assurance of a user's personal identifier(s) and privilege(s) in a secure, efficient and cost effective manner. Biometric identity management is concerned with the large-scale management of the biometric identities for an enrolment population. A narrow view is traditionally based on the enrolment step and the authentication step:

Identity Registration. A robust enrolment process is the main function that every authentication system must provide. A weak enrolment process will lend inaccuracies in the system and an unreliable authentication infrastructure. Ideally, a good enrolment process is one in which the credentials of the user are properly checked at the enrolment stage. An enrolment process where neither party can repudiate their participation in the transaction is the best way to address the quality of data and maintain a robust identification process;

Identity Assurance. Identity management solutions must assert an individual's identity to the applications running in a system/platform. There are two main methods for user recognition:

- *Verification* is the process verifying an individual's identity based on the presentation of a claim with one or more biometric features. For a given claim, the system matches the presented biometric data against the corresponding previously stored, labelled data and returns a matching identification score;
- *Identification* is the process verifying an individual's identity without the use of a claim: user identification is performed processing the entire enrolled population (database) and giving a matching identification score for each item. The highest matching identification score will label the processed feature. Identification is usually used for small populations or subsets of people;

Identity Protection deals with the protection and the integrity of an individual's identity. A simple biometric reader installed in a workstation in a protected environment does not represent a secure infrastructure: this can be a very dangerous practice since their security is weak. A secure approach involves the encrypting of biometric data during both the enrolment and verification phases, as well as the security countermeasures listed in the previous section.

3. Techniques for fingerprint recognition: Past approaches

A fingerprint is composed of ridges and valleys which form unique geometric patterns in the skin [1]. Parallel ridge lines are characterized by end points and bifurcations, called minutiae. Minutiae are referred as micro features of a fingerprint image. At the same time, fingerprints are characterized by regions where the ridge line flow is irregular. *Delta* and *core*, called macro features, offer the most frequently used information. With more details, the core point is the centre of a circular edge pattern on a fingerprint image, and the delta point is the centre of a triangular edge pattern.

In literature many approaches have been proposed for developing fingerprint recognition systems. Generally, they are characterized by three main steps: image acquisition, biometric signature extraction, and matching between the acquired biological signature and the stored correspondent one. Fingerprint recognition systems have been divided into two main classes. The first class of systems uses micro-feature (minutiae) information to perform fingerprint matching [3], while the second class of systems uses macro-feature (core and delta) information to perform fingerprint classification [4]. There are not examples of fingerprint recognition systems based on core and delta points, since they exclude a whole fingerprint class (i.e. the Arch class does not contain the core and delta points). In [1–4] interesting software algorithms for fingerprint identification, verification and classification are described. In [5], an algorithm for fingerprint image enhancement is illustrated. In [6,7] two hardware fingerprint recognition systems are presented. However, in [6], the fingerprint matching phase has not been developed. In [8] a complete embedded fingerprint recognizer is proposed and prototyped using the Hamster Secugen sensor for image acquisition and the Celoxica RC1000 board, employing a Xilinx VirtexE2000 FPGA, for image processing and analysis.

In what follows, both minutiae and singularity point-based techniques are described.

3.1. Minutiae-based recognition techniques

Minutiae extraction is a very critical and complex task. Consequently, different dedicated algorithms had been proposed in literature [1–3]. Generally, the fingerprint recognition task is performed through the following phases:

- fingerprint image pre-processing phase;
- minutiae extraction phase;
- matching phase.

3.1.1. Fingerprint preprocessing phase

This phase aims to reduce authentication faults in terms of falsely accepted users and falsely rejected users. The most used pre-processing steps are: normalization and segmentation, directional image extraction, image binarization and thinning. In what follows, each step is briefly described.

Normalization and Segmentation: this step is performed to force original fingerprint gray levels (Fig. 1a) to admit an average value within a desired variance [20,21]. The segmentation step returns the uncorrupted fingerprint regions, while the corrupted and unrecoverable regions are erased (Fig. 1b);

Directional map extraction: the directional map is an image where each element represents the ridge orientation [5]. Using differential operators, such as the Sobel or Roberts operators, the gradient of the image intensity is evaluated. Subsequently, the gradient mean squared method [22] can be used to calculate the ridge angle (Fig. 1b);

Image Enhancement: enhancing the image aims to obtain a better ridge definition and reduce the noise caused by the acquisition process. The Gabor filter, applied on the gray-level fingerprint image, performs texture segmentation (Fig. 1c) [5];

Binarization: this process aims to obtain a binary image, where pixels can assume a binary value [1]. Generally, image binarization is performed applying an average filter to reduce image noise and a thresholding operation to determine binary pixels (Fig. 1c);

Thinning: this phase aims to reduce ridge thickness to the unitary value (Fig. 1d) [16].

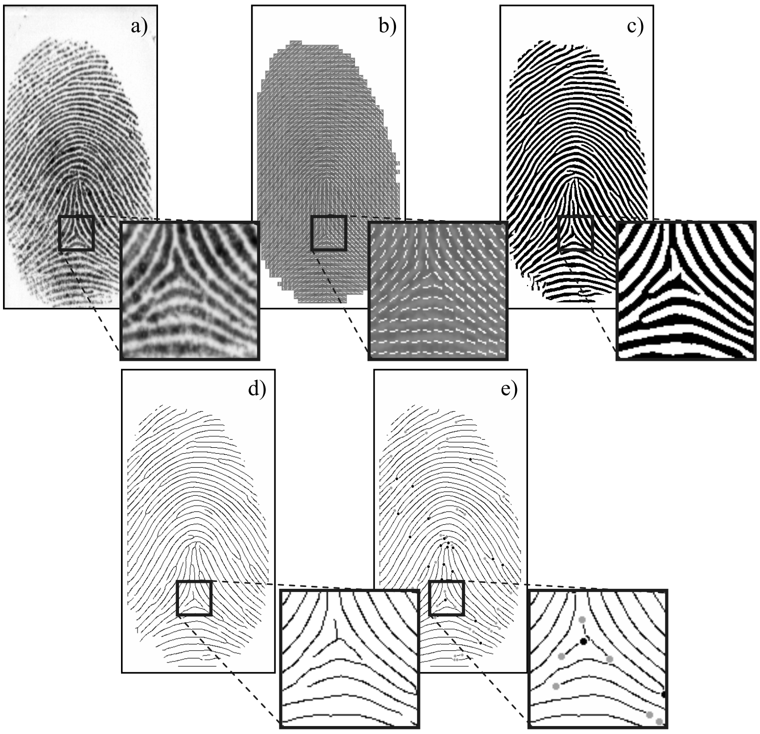


Fig. 1. Fingerprint processing steps: a) original fingerprint image; b) normalized and segmented fingerprint image with the overlapped directional image; c) enhanced fingerprint image using the Gabor filter, d) thinned fingerprint image, e) detected minutiae.

3.1.2. *Fingerprint minutiae extraction phase*

Usually, two procedures are used for minutiae extraction. The first procedure is devoted to minutiae analysis (i.e. ending points and bifurcation points classification) and localization, while the second procedure is devoted to the false minutiae erasing process. For each detected minutia, the resulting spatial coordinates and the orientation of the associated ridge are used to generate fingerprint template (Fig. 1e).

3.1.3. *Fingerprint templates matching*

A matching algorithm is required to find the correspondence between a processed fingerprint image and one or more stored templates. An enrolment phase aims to create one or more certified templates containing minutiae information for each user accessing a system/platform. The matching phase is devoted to assigning a similarity (matching) score to each template pair comparison.

Several algorithms are available for fingerprint template matching [1,3,4]. However, they can be classified into two main categories:

- *minutiae-based techniques*: these methods are based on the minutiae spatial coordinates comparison as well as on the comparison of the orientation angle of the ridge associated with the minutiae pair. Matching results are sensitive to image quality, since low quality images are characterized by considerable noise generating several false minutiae;
- *correlation-based techniques*: this approach takes into account the global pattern of ridges and valleys [3]. However, correlation-based techniques require one or more accurate points to register the fingerprint image with roto-translation operations [23].

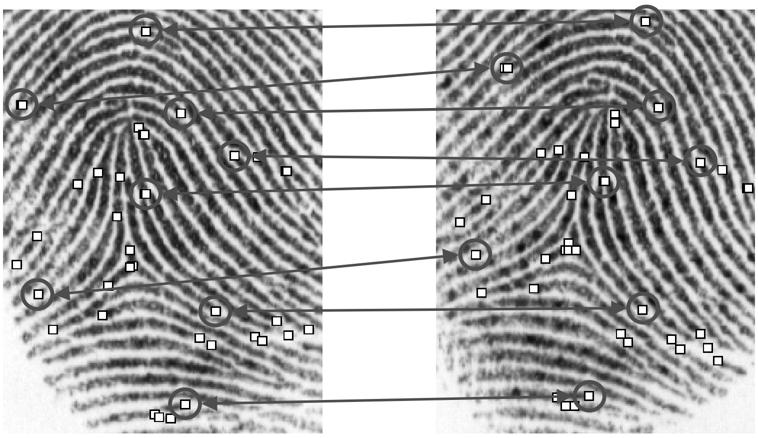


Fig. 2. Fingerprint minutiae-based matching. The figure illustrates two portions of a processed pair: squares are related to the detected minutiae; circles, connected by arrows, are related to a positive matched minutiae pair.

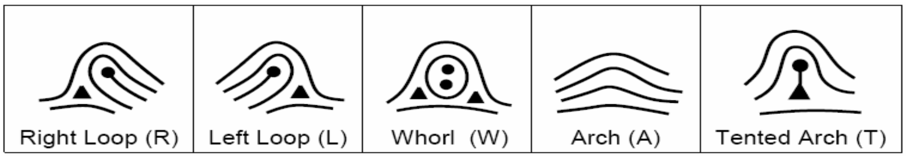


Fig. 3. The five NIST fingerprint standard classes: right loop (R), left loop (L), whorl (W), arch (A) and tented arch (T). Each class is characterized by 0, 1 or 2 core points and 0, 1 or 2 delta points.

3.2. Singularity points-based classification techniques

The National Institute of Standards and Technology (NIST) has classified human fingerprints in five classes. As depicted in Fig. 3, each class is characterized by n core and m delta, where $n =$ 0,1,2 and m = 0, 1, 2.

Fingerprint core and delta are also referred to as singularity points, used for fingerprint classification tasks [4]. Generally, the singularity points extraction is performed using three sequential steps: directional image extraction, computation of the Poincarè index and core and delta extraction. In succession the fingerprint image is classified using topological and numerical considerations (Fig. 3).

In the past singularity points have not been used for fingerprint recognition, since these points are difficult to find in ink-on-paper acquired fingerprints, corrupted fingerprints, and so on. However, modern optical and photoelectric sensors give high quality fingerprint images with well-defined core and delta points, if they are present. As a result, a singularity points-based recognition system can be developed with medium-high quality databases as well as with on-line recognition systems.

Several approaches for the singularity point detection have been proposed in literature. They can be broadly classified in techniques based on (i) the Poincarè index, (ii) Heuristics, (iii) Irregularity or Curvature Operators, and (iv) Template Matching.

4. Multimodal biometric systems

The concept of this research approach is the inclusion of multiple biometric modalities in one authentication process. In general, the architecture of multimodal biometric system consists of several biometric

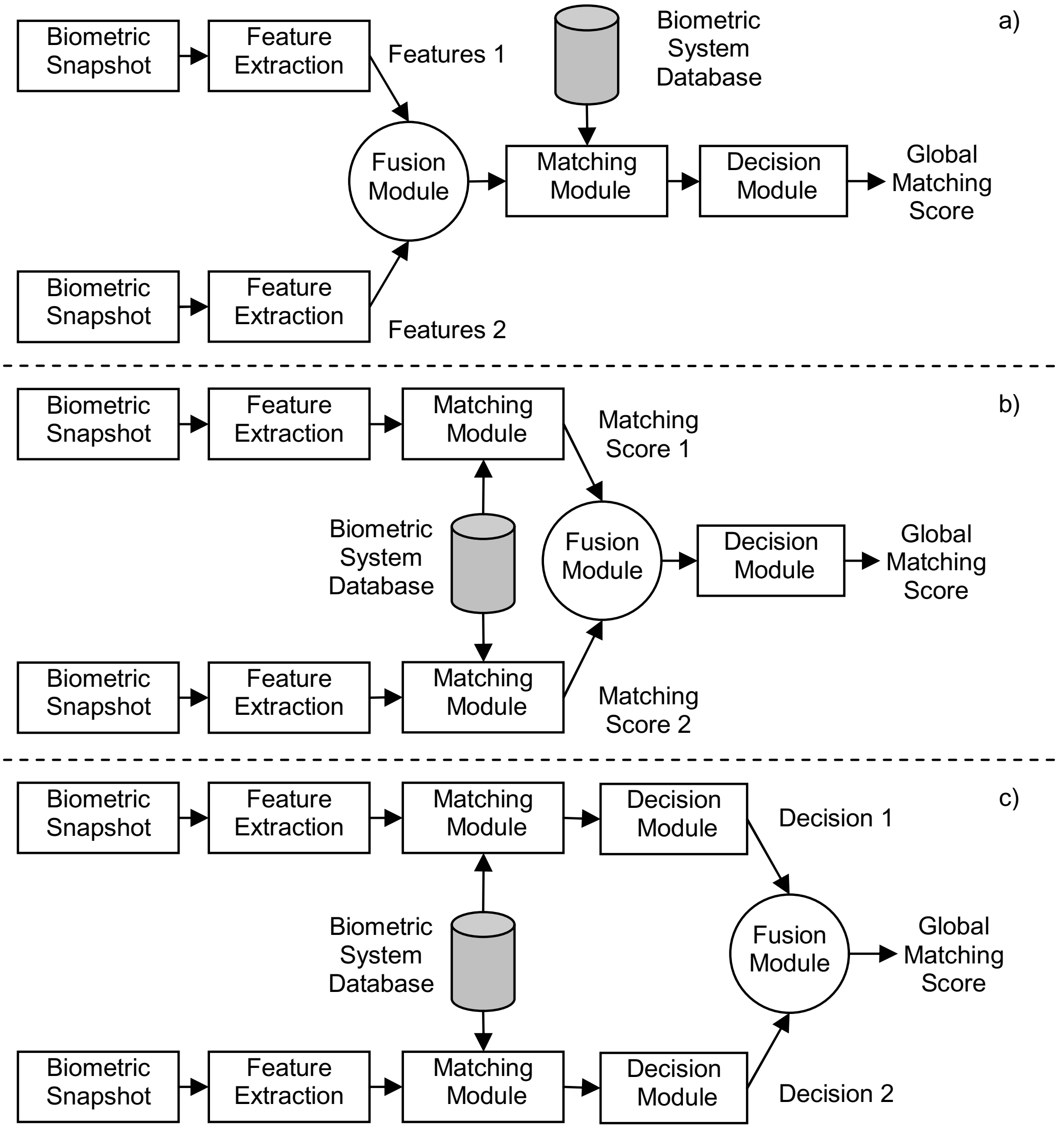


Fig. 4. Different fusion levels in a multimodal biometric system: a) fusion at feature extraction level; b) fusion at matching score level; c) fusion at decision level.

subsystems for different modalities [18,19]. Each subsystem consists of a data acquisition module, a pre-processing module, a feature extraction module, and a recognition module. Module type and presence depends on the fusion strategies of the multimodal biometric system. Generally, a multimodal biometric system can be based on three alternative fusion levels: feature extraction level, matching score level and decision level (see Fig. 4).

4.1. Different strategies for data fusion

The fusion strategies (see Fig. 4) are divided into two main categories: pre-mapping fusion (before the matching phase) and post-mapping fusion (after the matching phase). The first strategy deals with feature vector fusion level. These techniques are not used because they give many implementation problems. The second strategy is made possible by the decision fusion level, based on some algorithms which combine single decisions for each component of the system. Alternatively, the third strategy is based on the matching score fusion level, which combines the matching scores of each component system. The biometric data can be combined at several different levels in the recognition process. Inputs can be merged in the following levels [18,19]:

- *fusion at the feature extraction level:* the information extracted from sensors of different modalities is stored in feature vectors, on the basis of their modality. These feature vectors are then combined with a joint feature vector, which is the basis for the matching and recognition process. One of the potential problems in this strategy is that, in some cases, a very high dimensional feature vector results from the fusion process.
- *fusion at the matching score level:* this process is based on the combination of matching scores, after separate feature extraction and comparison between stored data and test data has been calculated for each subsystem. Starting from the matching scores or distance measures of each subsystem, an overall matching score is calculated using linear or non-linear weighting.
- *fusion at decision level*: with this approach each biometric subsystem autonomously completes the processes of feature extraction, matching, and recognition. Decision strategies are usually of a Boolean nature, where the recognition yields the majority decision among all present subsystems.

5. The proposed multimodal technique for identity management

An Automatic Fingerprint Authentication System (AFAS) consists of three main processing steps: image acquisition, features extraction, and biometric templates matching. In the first phase, a sensor scans and acquires the fingerprint image. Successively a vector of features, containing information about the micro and/or the macro features will be extracted. In many cases, this step is preceded by a pre-processing phase allowing fingerprint image quality to be enhanced. Finally, a matching score is used to quantify the similarity degree between the input image and the stored templates. Generally, a threshold-based process is used to accept or reject a user.

In this work, the authors propose a multimodal approach to design an AFAS whose performance in terms of FAR and FRR, lead to an usable recognizer in mobile payment systems. As pointed out before, a typical multimodal authentication system is composed of two or more parallel unimodal systems and a fusion module processing each single system output.

The proposed system architecture is composed of two AFAS modules based on micro and macro features, respectively. Result fusion is made possible by combining the matching score of both AFASs (Fig. 4b) in order to obtain an overall matching score. As depicted in the Fig. 5, an acquired fingerprint image is processed by the *Fingerprint Singularity Points Extraction Module* in order to extract useful information (presence, number, and position) on core and delta point.

Fingerprint image as well as singularity point information are used as inputs of both *Micro-Characteristics-Based Authentication Module* (*MicroCBA Module*) and *Macro-Characteristics-Based Authentication Module* (*MacroCBA Module*). The *MicroCBA Module* uses singularity point information for fingerprint registration and performs fingerprint template matching using minutiae type and position (micro-features). The *Macro-CBA Module* performs fingerprint template matching using only the directional image of the original fingerprint and the information generated by the singularity points. Both modules perform fingerprint template matching after the stored template decryption, since the fingerprint

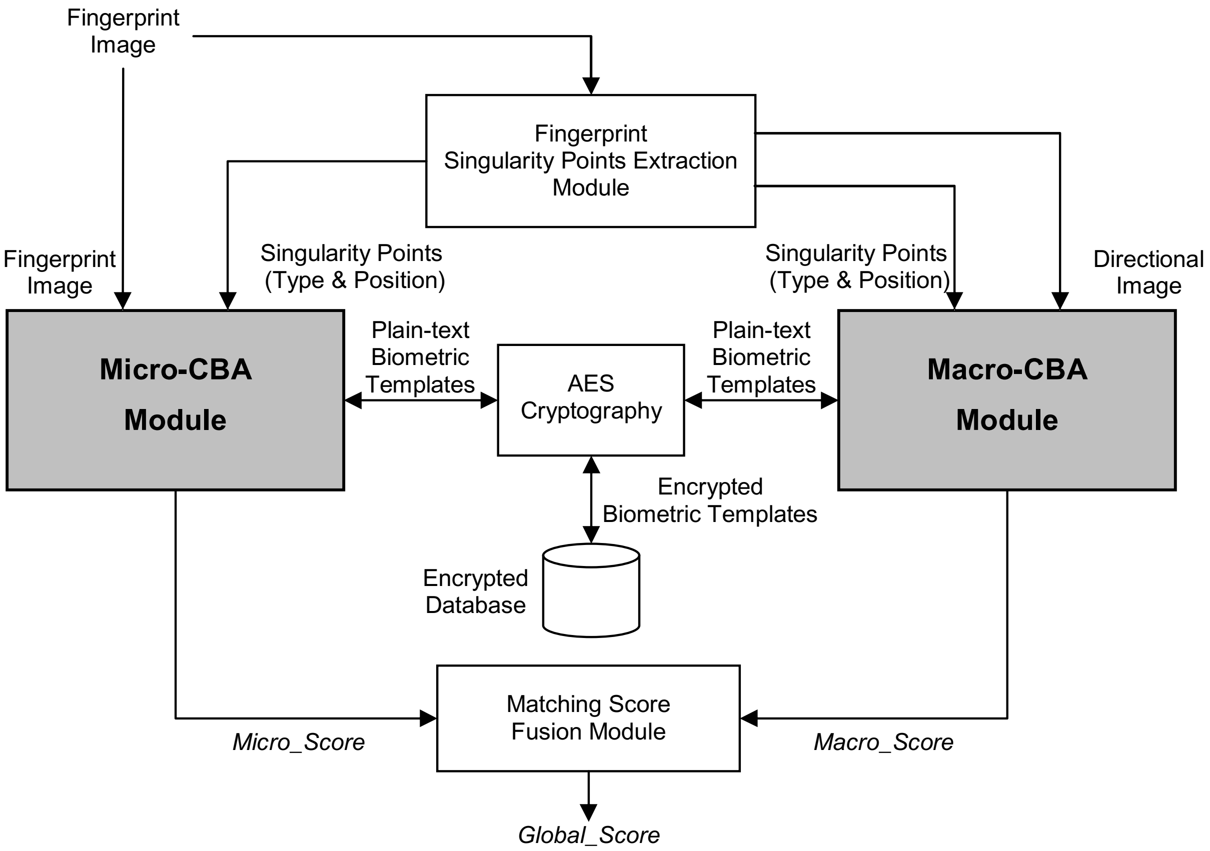

Fingerprint Image
Fingerprint Singularity Points Extraction Module
Fingerprint Image
Singularity Points (Type & Position)
Singularity Points (Type & Position)
Directional Image
Micro-CBA Module
Plain-text Biometric Templates
AES Cryptography
Plain-text Biometric Templates
Macro-CBA Module
Encrypted Biometric Templates
Encrypted Database
Matching Score Fusion Module
Micro_Score
Macro_Score
Global_Score

Fig. 5. The entire block scheme of the proposed multimodal authentication system. The gray blocks draw attention to the main modules of the proposed system: the Micro-Characteristics-Based Authentication Module (MicroCBA Module) and the Macro-Characteristics-Based Authentication Module (MacroCBA Module).

templates are encrypted before their storage. The unimodal matching scores are finally combined to obtain the overall matching score. However, singularity points detection can fail, since fingerprints can be corrupted, broken or the fingerprint is missing the core and delta points (i.e. it belongs to the Arch class). In this case, the *Micro-CBA Module* performs fingerprint templates matching using only minutiae information without fingerprint registration, while the *Macro-CBA Module* will give zero as matching. For this reason, the overall matching score is obtained using different weights for the two AFASs.

5.1. Fingerprint singularity points extraction module

Module functionality is related to the singularity point information extraction. Singularity points detection is based on the values obtained by the Poincarè index, obtained from directional image of the original fingerprint. As depicted in Fig. 6, the task is composed of three steps: directional image extraction, Poincarè index computation, and singularity points extraction. Directional image extraction is composed of four sequential modules: (i) Gx and Gy gradients computation using Sobel operators; (ii) Dx and Dy derivatives computation; (iii) θ(i,j) angle computation; (iv) Gaussian smoothing filter application on angle matrix [10]. Finally, the singularity points are detected using the Poincarè index, computed by taking the sum of the orientation changes along a closed curve around the pixel of interest. The extracted directional image represents a module output, too (see Figs 5 and 6).

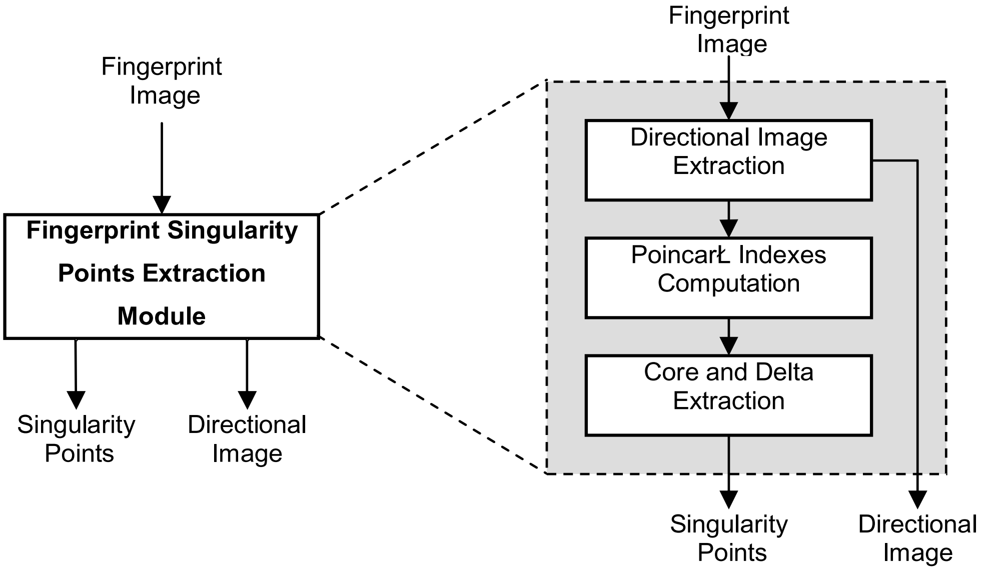

Fingerprint Image
Fingerprint Singularity Points Extraction Module
Singularity Points
Directional Image
Fingerprint Image
Directional Image Extraction
PoincarŁ Indexes Computation
Core and Delta Extraction
Singularity Points
Directional Image

Fig. 6. The processing scheme of the Fingerprint Singularity Points Extraction Module.

5.2. Micro-CBA module

In Section 3.1, a minutiae-based recognition system has been analyzed and described. In our tasks, in order to reduce the acquired fingerprint noise, a pre-processing phase is needed. This phase aims to reduce authentication faults in terms of falsely accepted users and falsely rejected users. The implemented pre-processing steps are: image segmentation, image enhancement using a Gabor filter, and thinning:

- *image segmentation*: this is achieved by using two complementary methods: the directional and the variance method [20,21]. The directional method shows a good behaviour either when it is applied to low contrast and noisy areas or when it is applied to regions containing clear ridges. The variance method shows a good behaviour when it is applied to high contrast areas. Furthermore, the above algorithms are able to split the background area and the foreground area, with the useful information.
- *image enhancement*: this filtering process is based on the well-known Gabor pass-band filter [5]. The Gabor filter enhances image quality, shifting the dark pixels towards the 0 (black) and the light pixels towards the 1 (white). It is applied in order to obtain visible and well-defined ridges;
- *thinning*: this step is performed to reduce ridge thickness to the unitary value using the Zhang-Suen algorithm [16]. Using a 3 × 3 moving kernel, each central pixel will be processed and its neighbourhood analyzed in order to label it as a candidate erasable pixel. At the end of this process, every candidate erasable pixel will be synchronously erased and the process restarts.

5.2.1. The matching algorithm

An ideally designed matching system should be immune from fingerprint translation, rotation and non-linear deformation issues. For this reason, singularity point information is checked before running the fingerprint template matching algorithm. As pointed out before, singularity point presence and position could be used for fingerprint pair registration before evaluating the matching score. However, if no singularity points are extracted, the template matching algorithm will be performed on the set of extracted minutiae without the registration step and without considerable reduction of the deformation problem.

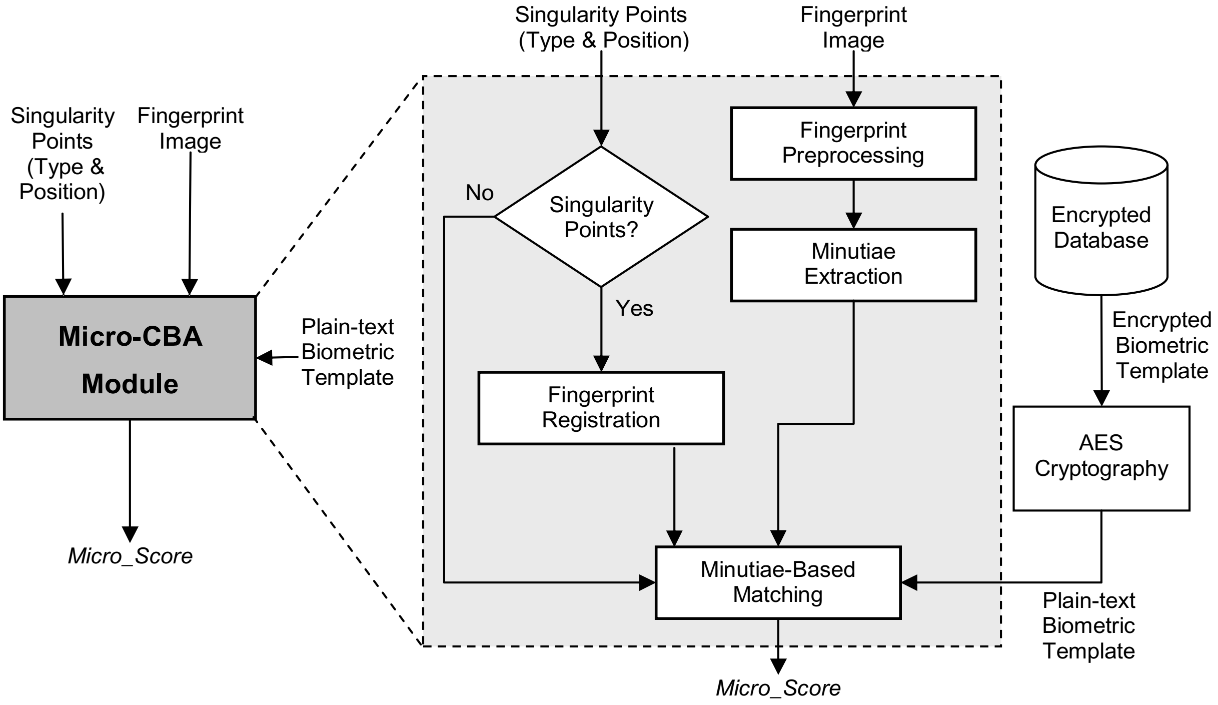


Fig. 7. The flow diagram of the Micro-CBA Module. Minutiae information, i.e. the output of the Minutiae Extraction block, is joined to the information coming out the Fingerprint Registration block, when fingerprint singularity points are detected. The Minutia-Based Matching block gives the similarity index about the processed fingerprint-template pair.

With more details, the template matching algorithm is based on the extracted micro-characteristics (minutiae spatial coordinates and ridge direction) and involves a fingerprint pair composed of the acquired fingerprint and a stored template. So, the on-line acquired fingerprint image is tentatively registered. Successively, a window, centred in the minutiae position, is considered to reduce deformation problems, when and only when core and delta points were detected. Finally a comparison between correspondent windows in each fingerprint pair is performed. The *Micro_Score*, (see Figs 5 and 7) will be the percentage of the correctly matched minutiae.

5.3. *Macro-CBA module*

Despite to the classical minutiae-based fingerprint authentication systems, this module is based on the fingerprint core and delta points. The block scheme of the designed system is depicted in Fig. 8. The proposed system exploits core and delta punctual and local information for fingerprint matching. With more details, the comparison between core and delta position, core and delta relative distance and orientation, and the information contained in their respective neighbourhoods are used for the similarity degree computation between the acquired fingerprint and one or more stored templates.

5.3.1. *The core and delta-based matching algorithm*

The proposed algorithm receives as input the coordinates of core and delta points and the directional image. If no singularity points have been detected and extracted, the matching score will be equal to zero. Otherwise, the singularity regions will be analyzed through (i) singularity regions analysis, and (ii) topological region analysis [10]:

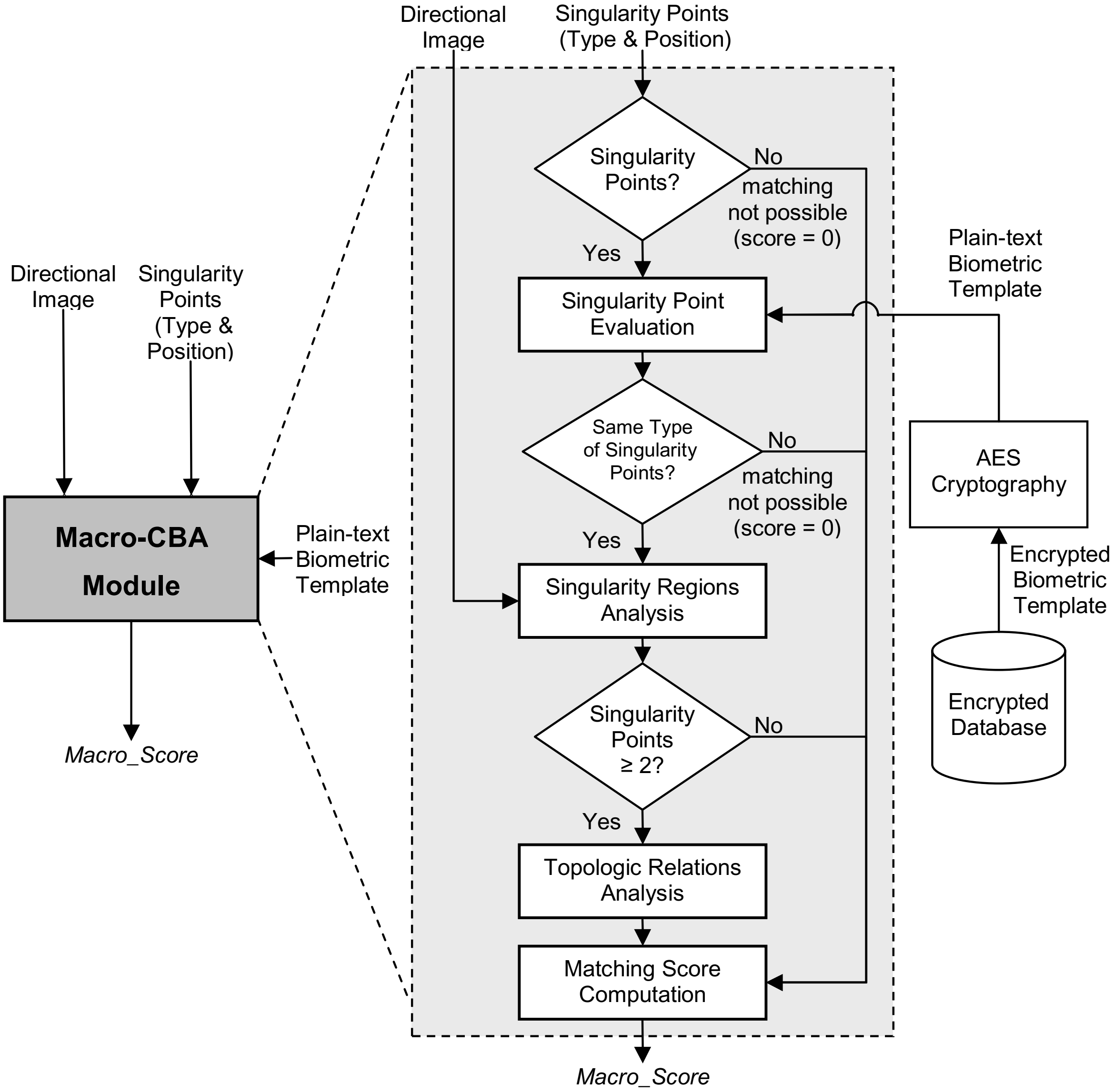

Directional Image
Singularity Points (Type & Position)
Macro-CBA Module
Plain-text Biometric Template
Macro_Score
Directional Image
Singularity Points (Type & Position)
Singularity Points?
No
matching not possible (score = 0)
Yes
Singularity Point Evaluation
Same Type of Singularity Points?
No
matching not possible (score = 0)
Yes
Singularity Regions Analysis
Singularity Points ≥ 2?
No
Yes
Topologic Relations Analysis
Matching Score Computation
Macro_Score
Plain-text Biometric Template
AES Cryptography
Encrypted Biometric Template
Encrypted Database

Fig. 8. The flow diagram of the Macro-CBA Module. Depending on the number and the type of the detected singularity points, the Singularity Regions Analysis block and the Topologic Relations Analysis block give their contribution for the Macro similarity index about the processed fingerprint-template pair.

– *singularity regions analysis*: The algorithm receives the directional image and the decrypted stored template as inputs. If the fingerprint-template pair has at least two singularity points of the same type (core-core or delta-delta), the procedure starts with an error computation, depending on the two directional image differences. Equations (1), (2) and (3) show how the similarity index is built, starting from the sum of the absolute values of the difference between the corresponding directional image angles (see Fig. 9). In the Eqs (1), (2) and (3), K_1, K_2 and K_3 are experimental constants, while $d_{Test}(i,j)$ and $d_{Template}(i,j)$ represent the angles of the directional images in the core (delta) neighbourhood.

Table 1
The three weights for the error measures in the macro-CBA module. The measures come from the core analysis procedure, delta analysis procedure, and topological relation analysis procedure

Process	Core analysis	Delta analysis	Topological relation analysis
Weight value	0.35	0.20	0.45

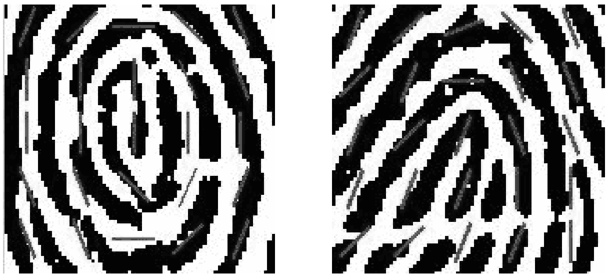


Fig. 9. The directional image of detected singularity regions overlapped with the fingerprint image.

$$m = \sum_{i=1}^{5} \sum_{j=1}^{5} |d_{Test}(i,j) - d_{Template}(i,j)| \tag{1}$$

$$error = K_1 \times (e^{(K_2 \times m)} - 1) \tag{2}$$

$$similarity = K_3 - error \tag{3}$$

– *topologic relations analysis*: If the fingerprint-template pair has at least four singularity points, the procedure starts selecting singularity point neighbourhoods with the minimum relative distance (the minimum distance is chosen to reduce distortion effects.) The Euclidean distances between the same type of singularity points (core-core or delta-delta) are then calculated. If these distances are under a certain tolerance threshold (reduced distortion effects), all possible relative distances between the selected singularity points are computed and analyzed to extract the error measure (resulting in the selection of the pair with the lower error). Further details on this method are reported in [10]. Since the distance between two singularity points is invariable with respect to the roto-translations variations, the singularity points extraction can be performed without an images registration phase.

The previous error measures are then combined to obtain the overall Macro_Score index. Since the procedures and techniques to obtain the single error measure are different, a weighted sum of these errors is implemented, using the values depicted in Table 1, to obtain the overall Macro_Score index (the analysis on topological relations gives the highest contribution since it involves topological information of the core and delta regions).

5.4. AES fingerprint template encryption/decryption module

To increase security, biometric templates are encrypted using the AES (Advanced Encryption Standard) algorithm that is a particular case of the Rijndael algorithm [17]. In the AES, the input plain-text is divided in blocks of fixed dimensions, while algorithm keys have different length. The AES uses matrixes of same block dimensions. The encryption process is divided into several iterations (Fig. 10a). In the decryption process (Fig. 10b), the same steps are performed using the inverse transformations tables: starting with the ciphered-text as input, the plain-text is obtained as output.

Table 2
Recognition results of the unimodal Micro-CBA module, of the unimodal Macro-CBA module, and of the final multimodal system

Authentication rates on FVC database		
	FAR (%)	FRR (%)
Macro-CBA Module	2.56	18.92
Micro-CBA Module	1.52	20.35
Multimodal System	1.07	10.71

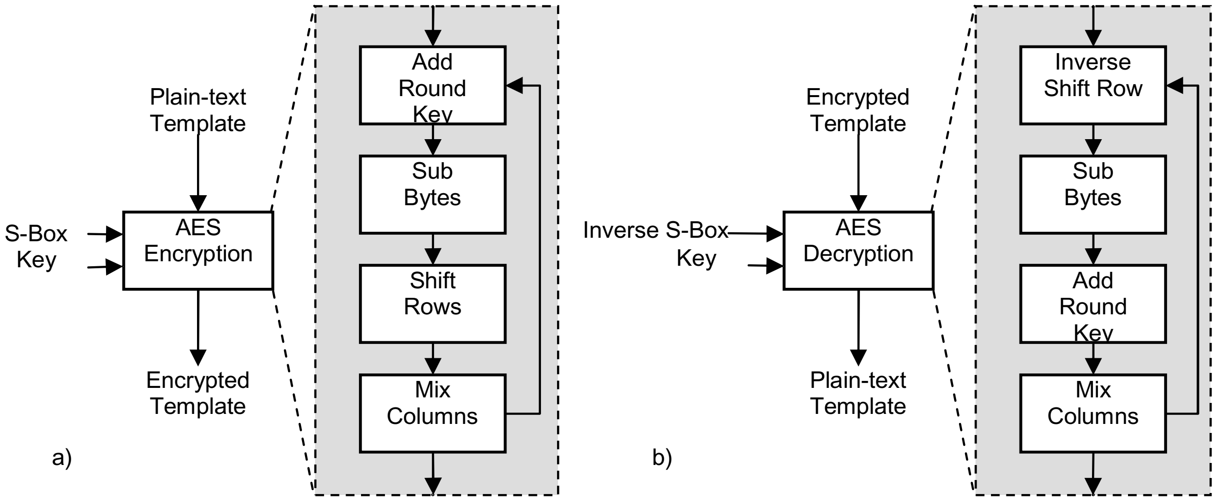


Fig. 10. (a) Encryption and (b) Decryption block schemes of the AES algorithm.

5.5. The matching score level fusion module

The *Matching Score Level Fusion Module* computes the overall matching score combining the two unimodal subsystem matching scores. Since the *Micro-CBA Module* and the *Macro-CBA Module* are based on different techniques and parameters to determine the unimodal matching score, a weighted sum (with two different weights) has been used to obtain the overall matching score. Experimental trials have demonstrated that the best performance, in terms of FAR and FRR indexes, is obtained with the following Eq. (4), where 0.6 and 0.4 have been experimentally optimized.

$$Global\_Score = 0.6 * Micro\_Score + 0.4 * Macro\_Score \tag{4}$$

6. Multimodal system recognition rates

Biometric system evaluation has been performed using the FAR and FRR indexes. The FVC2002/DB2 database [31] which was utilized is composed of gray scale fingerprint images captured by an optical sensor. This database is composed of 80 images of 296 × 560 pixels, collected from 10 people (8 acquisitions for each person).

Table 3 shows the FAR and FRR indexes obtained by the micro-CBA module and the macro-CBA module, respectively. In the same table the FAR and FRR indexes of the multimodal system are also listed. FAR and FRR of the Micro-CBA Module have been obtained using 12 coinciding minutiae for

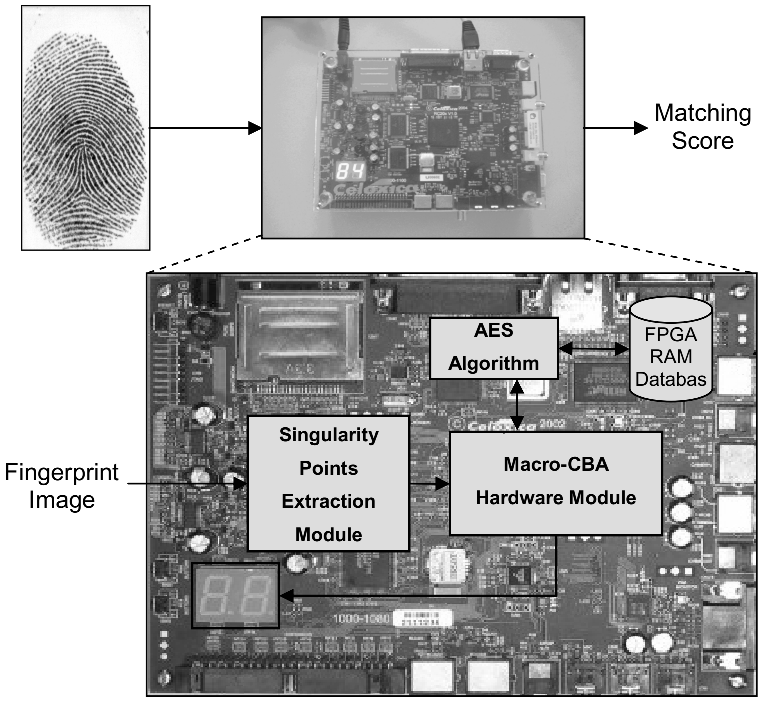

Matching Score
AES Algorithm
FPGA RAM Databas
Singularity Points Extraction Module
Macro-CBA Hardware Module
Fingerprint Image

Fig. 11. The proposed embedded recognizer implemented using the FPGA technologies available on the Celoxica RC203E board. In bold are highlighted the implemented hardware modules: the Singularity Points Extraction Module, and the Macro-CBA module. The Macro_Score is visualized through the 7-segments display.

each processed fingerprint pair, as suggested by FBI [32]. FAR and FRR of the Macro-CBA Module have been computed when 60% of the directional field of each processed pair coincides. Table 2 shows that the multimodal approach reduces the false acceptance rate and halves the false rejection rate.

7. Prototyping a self-contained fingerprint recognizer

The objective of the embedded approach is to overcome some of the limits of the software fingerprint recognition systems.

In this work, the authors have implemented a biometric sensor that is able to acquire a fingerprint image, process it and, select (in the matching phase) the corresponding database item for individual authentication (see Fig. 11). In the current implementation, the prototyped sensor implements only the Macro-CBA Module. With more details the core and delta singularity extraction module and macro-characteristics-based authentication module has been described and synthesized using Handel-C language [29], Celoxica DK4 [27] and the Xilinx ISE [28] development environments. The implementation shows that the macro features approach offers an excellent compromise between resource utilization and recognition rates.

7.1. System description

The proposed mobile biometric recognizer, considering all its functionalities, is composed of three main modules. The Fig. 12 shows the interactions between the three modules:

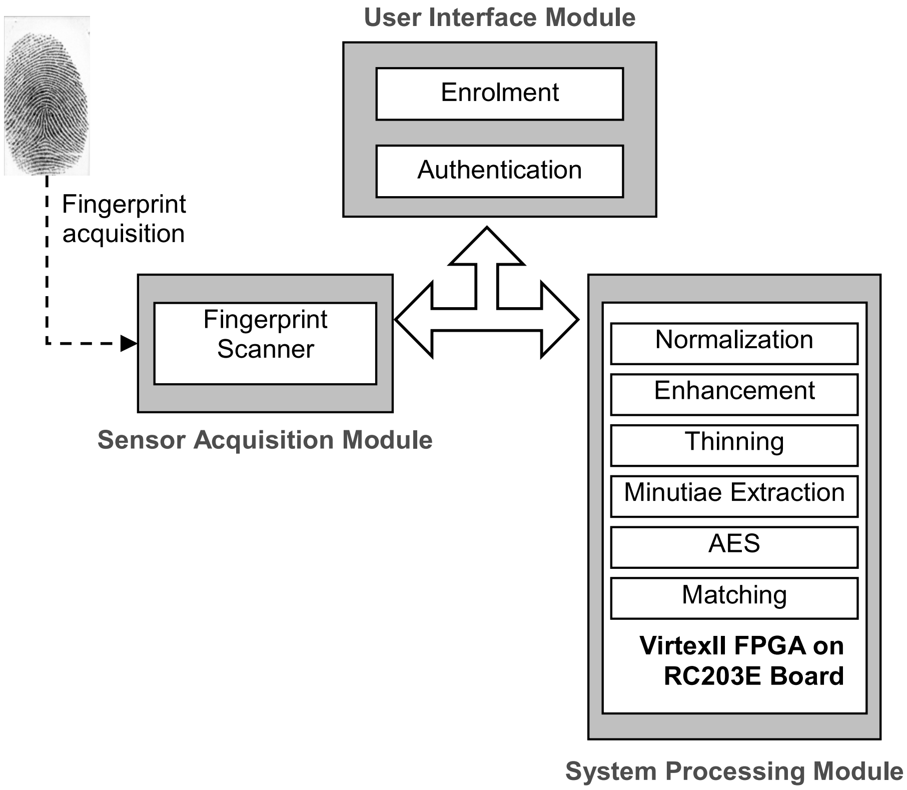


Fig. 12. The three main modules of the embedded recognizer: the UIM (User Interface Module), the SPM (System Processing Module), and the SAM (Sensor Acquisition Module).

- *UIM* (*User Interface Module*): has been expressly developed for providing the interface necessary for the user in the authentication process;
- *SPM* (*System Processing Module*): has been implemented on the Celoxica RC203E board and performs all the steps of the fingerprint processing chain. It represents the engine of the recognizer;
- *SAM* (*Sensor Acquisition Module*): manages the Biometrika FX2000 optical scanner during the fingerprint acquisition phase.

7.2. Experimental results

The obtained experimental results, in terms of resources analysis, execution times and recognition rates are here outlined.

7.2.1. Database properties description

The proprietary database which was utilized is composed of gray scale fingerprint images captured by the Biometrika FX2000 optical scanner [30]. This database is composed of 75 images (25 users) of 296 $\times$ 560 pixels.

7.2.2. Hardware execution times

The algorithms implementation on FPGA allows the simultaneous performance of these highly competitive systems. The proposed recognition system takes advantage of FPGA technologies and introduces

Table 3
Execution times for each phase of the implemented sensor, The working frequency is 25.175 MHz

System module	Execution time (ms)
Pre-processing phase and core and delta extraction	31.20
Matching algorithm	3.62
Total time	34.82

Table 4
Xilinx VirtexII XC2V3000 required resources

Resource Type	Available	Used	Usage (%)
FLIP FLOPs	28,672	5,138	17.91
SLICEs	14,336	12,863	89.72
LUTs	28,672	20,825	72.63

Table 5
Recognition results of the prototyped sensor on the proprietary CSAI Database

Database	FAR (%)	FRR (%)
CSAI Database	1.89	11.43

interesting characteristics considering the algorithms used and the performance achieved. Table 3 shows the elaboration times necessary to perform every single authentication task, with a working frequency of 25.175 MHz, is 34.82 ms. The low working frequency suggests interesting considerations for the employment of 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.

7.2.3. *Hardware resources analysis*

As pointed out before, the tools used for sensor prototyping are the Celoxica DK4 and Xilinx ISE for the development of the Handel-C description code. Table 4 shows the FPGA physical resources available which were used for the design implementation. With more details, the number of FLIP FLOPs, SLICEs (logical cells contained in the Configurable Logic Block), LUTs (Look-Up Table used as boolean function generator) are listed in Table 4. The used resources give ample room to implement the whole multimodal system on the FPGA-based board.

7.2.4. *Hardware recognitions rates*

The evaluation of the performance of the embedded recognizer has been performed by utilizing the FAR and FRR indexes. Table 5 lists the best trade-off achieved in our trials. Similar results have been achieved on a set of 413 fingerprints randomly extracted from FVC databases [10].

8. Conclusions

Ubiquitous networks and mobile applications are creating a revolution in the way people live by providing a vast array of distributed services and functionalities in a wide range of arenas. A ubiquitous and mobile communication environment needs many self-contained authentication sensors, opportunely distributed, for user recognition and the secure access of the consumer to services, such as mobile payment systems.

In this paper a multimodal biometric system, combining two fingerprint authentication systems based on fingerprint minutiae and singularity points, is proposed. The multimodal biometric system has been tested on the official FVC2002/DB2 database [31] where an interesting working point was reached when the FAR is 1.07% and the relative FRR is 10.71%. In addition, a hardware fingerprint recognizer has been prototyped to design a self-contained sensor for use in mobile payment systems. With this approach, fraud and authorization risk to mobile operators can be greatly reduced. The low working frequency (25.175 MHz) and the low execution time (34.82 ms) suggest its easy utilization by portable devices.

References

[1] V. Conti, G. Pilato, S. Vitabile and F. Sorbello, *A Robust System for Fingerprints Identification, Knowledge-Based Intelligent Information Engineering System and Allied Technologies*, Crema 16–18 September 2002, 1162–1166.

[2] V. Conti, G. Pilato, S. Vitabile and F. Sorbello, *Verification of Ink-on-paper Fingerprints by Using Image Processing Techniques and a New Matching Operator*, AI*IA Siena, 10–13 September 2002, 594–601.

[3] A.K. Jain, On-Line Fingerprint Verification, *IEEE Transaction on Pattern Analysis and Machine Intelligence* **19**(4) (1997), 302–314

[4] S. Prabhakar, A.K. Jain and W. Jianguo, *Minutiae Verification and Classification*, Department of Computer Engineering and Science, University of Michigan State, East Lansing, MI 48824, 1998.

[5] L. Hong, Y. Wan and A. Jain, Fingerprint Image Enhancement, Algorithm and Performance Evaluation, *IEEE Transaction on Pattern Analysis and Machine Intelligence* **20**(8) (1998), 777–789.

[6] V. Bonato, R.F. Molz, J.C. Furtado, M.F. Ferrão and F.G. Moraes, Propose of a hardware implementation for fingerprint systems", UNISC – Departamento de Informatica Santa Cruz-Brazil, PUCRS – Faculdade de Informatica porto Alegre – Brazil.

[7] P. Schaumont and I. Verbauwhede, *ThumbPod Puts Security Under Your Thumb*, Xilinx Xcell Journal, October 2003 (Winter 2004), EE Department, UCLA.

[8] S. Vitabile, V. Conti and F. Sorbello, An Embedded Fingerprint Recognizer, in: *Embedded Systems: Status and Perspective*, Z. Shao, Y. Zhang and L. Tang, eds, American Publishers.

[9] S. Vitabile, V. Conti, G. Lentini and F. Sorbello, *An Intelligent Sensor for Fingerprint Recognition*, Proc. of International Conference on Embedded And Ubiquitous Computing (EUC-05), Lecture Note in Computer Science (LNCS), Springer-Verlag, Vol. 3824, pp. 27–36, ISBN 3-540-30807-5.

[10] C. Militello, V. Conti, S. Vitabile and F. Sorbello, *A Novel Embedded Fingerprints Authentication System based on Singularity Points*, proc. Of the International Conference on Complex, Intelligent and Software Intensive Systems (CISIS'08), pp. 72–78, March 4-7/2008, Barcelona, Spain, ISBN 0-7695-3509-1.

[11] H. Liu and C.-M. Zhang, *Research on Use of Distributed Authentication in Pervasive Computing*, 1st International Symposium on Pervasive Computing and Applications (SPCA06), 571–574.

[12] Y. Shuxin, R. Indrakshi and R. Indrajit, *A Trust Model for Pervasive Computing Environments*, 2nd International Conference on Collaborative Computing, 2006, (CollaborateCom 2006), 1–6.

[13] R. Sailer and J.R. Giles, *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), 144–148.

[14] Enabling secure, interoperable, and user-friendly mobile payments, *Mobile Payment Forum White Paper*, Mobile Payment Forum, 2002.

[15] UK Biometrics Working Group (BWG): *Biometrics Security Concerns*, 2003.

[16] T.Y. Zhang and C.Y. Suen: A fast parallel algorithm for thinning digital patterns, *Comm ACM* **27**(3) (1984), 236–239.

[17] J. Daemen and V. Rijmen, Aes proposal: Rijndael, citeseer.ist.psu.edu/daemen98aes.html.

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

[19] V. Claus, *Biometric User Authentication for IT Security from Fundamentals to Handwriting*, Springer-Verlag, 2006, ISBN 0-387-26194-X.

[20] B.M. Mehtre and B. Chatterjee, Segmentation of fingerprint images – a composite method, *Pattern Recognition* **22**(4) (1989), 381–385, ISSN:0031-3203.

[21] B.M. Mehtre, N.N. Murthy, S. Kapoor and B. Chatterjee, Segmentation of fingerprint images using the directional image, *Pattern Recognition* **20**(4) (1987), 429–435, ISSN:0031-3203.

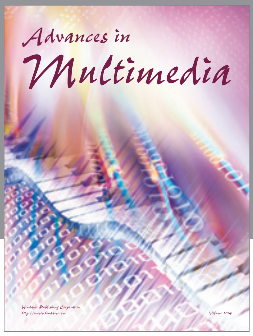
[22] A.R. Rao and B.G. Schunk, Computing oriented texture fields – Computer Vision and Pattern Recognition, Proceedings CVPR '89, IEEE Computer Society Conference on Digital Object Identifier.
[23] A.M. Bazen, G.T.B. Verwaaijen, S.H. Gerez, L.P.J. Veelenturf and B.J. van der Zwaag, *A Correlation-Based Fingerprint Verification System*, ProRISC 2000, Workshop on Circuits, Systems and Signal Processing, Veldhoven, The Netherlands, November 2000.
[24] A. Saxena, M.L. Das and A. Gupta, MMPS: a versatile mobile-to-mobile payment system, *International Conference on Mobile Business* ICMB (2005), 11–13, (July 2005), 400–405.
[25] H. Lu, F. Claret-Tournier, C. Chatwin and R.C.D. Young, M-Commerce Secured Using Web-Enabled Mobile Biometric Agents, International Conferences on Web Intelligence and Intelligent Agent Technology Workshops, *2007 IEEE/WIC/ACM* (5–12 November 2007), 480–483
[26] Celoxica website, http://www.celoxica.com.
[27] Celoxica DK4 Version 4: "DK Design Suite User Guide". Celoxica Inc. http://www.celoxica.com/support/documentation.
[28] Xilinx Website, http://www.xilinx.com.
[29] Celoxica Handel-C Language Reference Manual, version 3.1, Celoxica Ltd. http://www.celoxica.com.
[30] Biometrika website, http://www.biometrika.it.
[31] FVC website, http://bias.csr.unibo.it.
[32] FBI website, http://www.fbi.gov/.

Vincenzo Conti is an Ph.D. of the Department of Computer Engineering in the University of Palermo, Italy. He received his "Laurea cum Laude" and his Ph.D. in Computer Engineering from the University of Palermo in 2000 and 2005, respectively. He collaborates currently both the Computer Science and Artificial Intelligence Laboratory of the Department of Computer Engineering and the Acoustics Laboratory of the Department of Energetic and Environmental Researches of the University of Palermo, Italy. His main researches regard the following fields: Biometric Recognition Systems; Intelligent Sensors for Biometric Recognition; Documents Retrieval; User Ownership in Multi-Agent Systems. In each of this research field he has produced many publications both national and international conferences and journals. Besides, Dr. Conti has participated to several research projects funded by industries and research institutes relative his research fields.

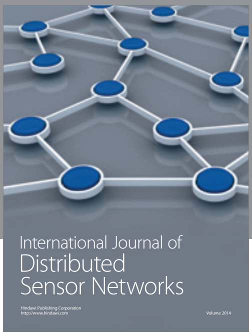
Carmelo Militello received his "Laurea" degree in Computer Engineering in 2006 from the University of Palermo, Palermo, Italy, with the following thesis: "A Dedicated System Based on Fingerprints and SmartCard for Users Authentication. Study and Realization on Programmable Devices Logical". Since January 2007 he is Ph.D. student in the Department of Computer Engineering (DINFO) of the University of Palermo. Militello is a component of the "Innovative Computers Architecture" (IN.C.A.) group of the DINFO, coordinated by the prof. Filippo Sorbello, and he is developing his scientific activity in the Laboratory of Electronic Calculators and Artificial Intelligence (CSAI). The principals research fields of Militello concerns with biometrics embedded systems, implemented on reconfigurable architecture as FPGA hardware devices.

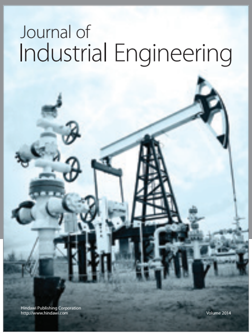
Filippo Sorbello is currently Full Professor in the area of Computer engineering (ING/INF-05 code) with the Department of Computer Engineering (Dipartimento di Ingegneria Informatica) of University of Palermo, Italy. He was the first Head of the same Department. He received the "Laurea" degree in Electronic Engineering in 1970 from the University of Palermo, Palermo, Italy. Since 1970 he has participated to several projects carried out by the Institutes and Departments in which he was involved. He was a CNR (Consiglio Nazionale delle Ricerche – Italian National Research Council) scholarship holder, regular assistant, delegate professor. Afterwards from 1982 he was Associate Professor of Computer Science at the University of Palermo and successively Full professor. His research interests are in the field of neural networks applications, real time image processing, biometric authentication systems, and multi-agent system security. Prof. Sorbello is an IEEE, ACM, AIIA and AICA member. He is the author of above 120 international scientific papers.

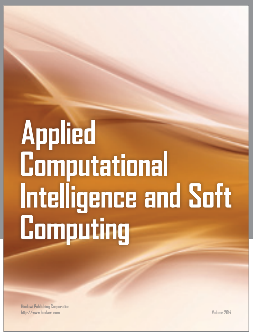
Salvatore Vitabile is an assistant professor with the Department of Medical Biotechnologies and Forensic Medicine, University of Palermo, Italy. He received the Dr. Ing. degree (M.S.E.E.) in Electronic Engineering and the doctoral degree in Computer Science from the University of Palermo in 1994 and 1999, respectively. Dr. Vitabile has participated to several research projects funded by industries and research institutes relative to Multi-Agent System security, time series analysis and forecasting, real-time video processing. Dr. Vitabile has co-authored more than 70 scientific papers in referred journals and conferences. He has served on organizing and program committees of international conferences, symposia, workshops and he is a reviewer for several scientific journals. He is a member of the Board of Directors of SIREN (Italian Society of Neural Networks), of IEEE, and IEEE Engineering in Medicine and Biology Society. His research interests include neural network applications, real-time image and video processing, application specific processors design and prototyping, biometric authentication systems, multi-agent system security, medical image processing.

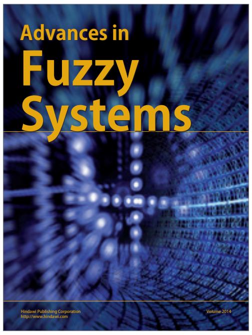

Advances in
Multimedia

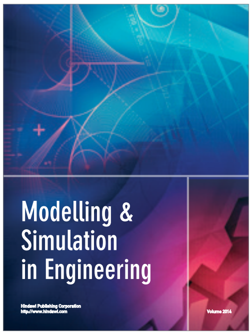
The Scientific
World Journal

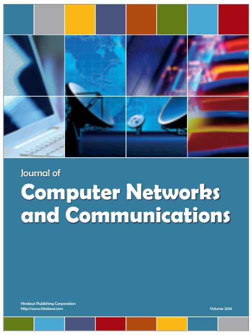

International Journal of
Distributed
Sensor Networks

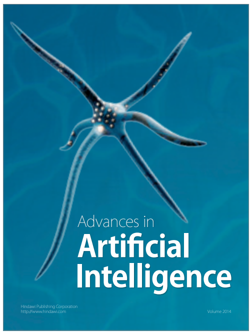

Journal of
Industrial Engineering

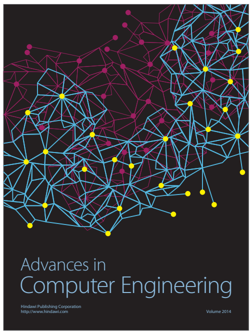

Applied
Computational
Intelligence and Soft
Computing


Advances in
Fuzzy
Systems

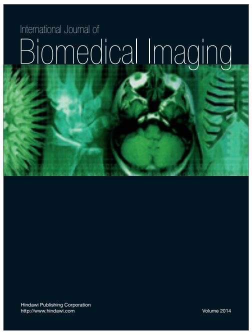

Modelling &
Simulation
in Engineering

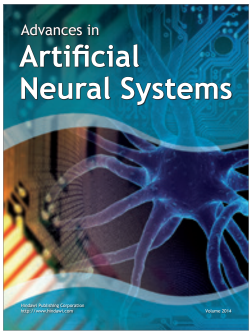

Journal of
Computer Networks
and Communications

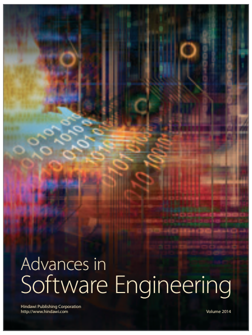

Advances in
Artificial
Intelligence


Advances in
Computer Engineering

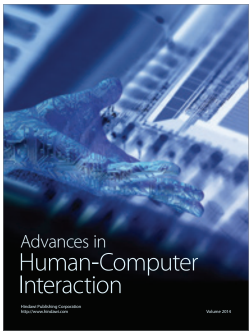
International Journal of
Computer Games
Technology

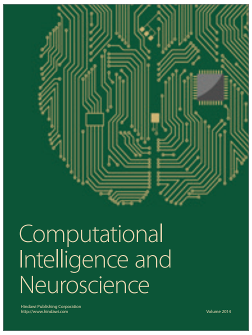

International Journal of
Biomedical Imaging


Advances in
Artificial
Neural Systems


Advances in
Software Engineering

Journal of
Robotics


Advances in
Human-Computer
Interaction


Computational
Intelligence and
Neuroscience

International Journal of
Reconfigurable
Computing

Journal of
Electrical and Computer
Engineering