MedCrave
Step into the World of Research
International Journal of Biosensors & Bioelectronics

Research Article
Open Access
CrossMark

Biometric authentication overview: a fingerprint recognition sensor description

Abstract

Biometrics provides an alternative paradigm for the personal authentication: our biological characteristics are unique and can be used to distinguish us from the other persons. Biometrics are automated methods of identifying a person or verifying the identity of a person based on a physiological or behavioral characteristic. Examples of physiological characteristics include hand or finger images, facial characteristics, and iris recognition. Behavioral characteristics are traits that are learned or acquired. Dynamic signature verification, speaker verification, and keystroke dynamics are examples of behavioral characteristics. In this paper a general overview of biometric systems based on the principal biometric technologies available and a description of a fingerprint recognition sensor performances are proposed. To test the biometric sensor performances two indexes are used, FAR (false accept rate) and FRR (false reject rate).

Keywords: sensor, biometric technologies, user security, recognition systems

Volume 2 Issue 1 - 2017

Vincenzo Conti,[1] C Militello,[2] S Vitabile[3]
[1]University of Enna Kore, Italy
[2]Institute of Molecular Bioimaging and Physiology, Italy
[3]Department of Biopathology and Medical Biotechnologies, University of Palermo, Italy

Correspondence: Vincenzo Conti, Faculty of Engineering and Architecture, University of Enna Kore,Viale delle Olimpiadi, 94100 Enna, Italy, Email vincenzo.conti@unikore.it

Received: December 27, 2016 | **Published:** January 26, 2017

Abbreviations: FAR, false accept rate; FRR, false reject rate; EER, equal error rate; ROC, receiver operating characteristic

Introduction

Today, the actual technological scenario provides advanced services to the user, neglecting a very important factor: the security. For example, it is necessary to remember a lot of passwords to access into our online banking account, or into our email box, ecc.[1] The standard authentication systems, based on username and password, are not able to assure a suitable protection level for the transmitted information. This authentication mechanism unfortunately is not sure: whoever can illegitimately know and reproduce the secret information that should guarantee only our access. The security user should be the main point of any software application dealing with personal information. The biometric science provides an alternative paradigm for the personal authentication: our biological characteristics are unique and can be used to distinguish us from the others person.[2]

In this paper a general overview of biometric systems and of the principal biometric technologies available is proposed and two indexes, FAR (false accept rate) and FRR (false reject rate), have been used to test the described fingerprint recognition sensor performances. The paper is organized as follow: in the section 2 are illustrated the possible modalities to user authenticate, considering the security issues related the biometric identity management; in the section 3 the principal functionalities and characteristics of a biometric system are analyzed, considering usability and problems; the section 4 introduces a set of existent available biometric technologies; in the section 5 the performance achievable from various biometric technologies are reported and finally some conclusions are reported.

Why biometrics?

In every authentication system, each user can use a service only if the following two security phases are performed

I. Authentication of the user digital identity.

II. Granting of rights to perform the desired action.

The authentication of the user digital identity is classified in the three following approach [3]

i. **Something that one knows:** if the user knows a pre-determined secret (generally represented by a password) then he is the correct person. In this system, the access is strongly conditioned by the password location: the probability that an impostor knows the password is high. This approach is called knowledge-based, because it uses information that only the user know.

ii. **Something that one has:** if a user possesses a pre-arranged token (magnetic badge or smartcard) then he is the correct person. The token proprietary should have full access, without asking other additional information. Also here, the access to the system, and therefore its safety state, is strongly conditioned by the token location. This approach is called token-based, because it uses information that the user possesses.

iii. **Something that one is:** in this approach, the concept is that the system compares user biometric characteristics with pre-registered values, known as template, allowing the access only if the measured characteristic corresponds to template stored in the system.

The more common authentication systems use the first and the second approach (or a their combination) to realize the user recognition. These kind of systems can be easily violated, simply stealing the token or knowing the password. These two approaches require that the user remember or carries with him "something" containing the necessary information for the authentication. With the third approach instead, the user haven't the necessity to remember or to carry with him nothing: all information necessary for authentication belong to the user. User physical and behavioral characteristics (as the face geometry, the iris and retina scansion, the fingerprints, the voice, the calligraphy and so on) constitute the core of biometric systems. The biometric identity has the advantage to assure that only the correct user can have access to determined services: only who

presents the correct physical characteristics will have guaranteed the access. A biometric system is based on a biometric characteristic, that cannot be stolen, and for this it is not easily violable. For example, if a smartcard containing the biometric template is stolen, nobody will can utilize it because its biometric data will not coincide with those stored on the smartcard. The system access will be denied.[3]

Biometric systems

A biometric system, using the digital technologies, can be used in two different ways

i. **Identification mode:** the user is identified by a database of people known to the system (who am I?).

ii. **Authentication mode:** The users declare his identity and the system verifies it (I am who say I am?).

A biometric system constitutes an automatic device for identification or authentication of the personal identity using its biological characteristics. The database, containing an digital representation (template) of the biometric characteristic, can be centralized or distributed. If the database is distributed, every user will possess a personal support, as a smartcard with own biometrics characteristics.[3]

In a authentication system, two different phases are performed

i. **Enrollment phase:** it is performed to insert the biometric characteristic in the system database. During this phase three specific operations are performed: biometric characteristic acquisition, digital biometric representation extraction and template storing in the database.

ii. **Verification phase:** it is effected every time that a user must be authenticated for accessing the system. Three operations are effected: biometric characteristic acquisition, biometric digital representation extraction, matching between the online acquisition biometric characteristics and the templates previously created in the enrollment phase.

Performance evaluation indexes

The biometric system performances can be valued considering the following main values:

I. The database dimension.

II. The system answers speed.

III. The accuracy about user recognition.

The template dimension, using smartcard for storage, is a principal issue in the selection of the biometric technologies type. The time employed by the system to take a decision is fundamental, especially in real-time applications. The recognition accuracy is the most important characteristics of the biometric recognition systems because it determines the system security.[4] The recognition performance is valued using two error indexes: the FAR, percentage of approved impostors, and the FRR, percentage of refused registered user. These two percentages are always calculated: for every FAR there is a relative FRR (Figure 1).

In a ideal biometric system these percentages would be both zero. Unfortunately, the ideal system doesn't exist and therefore it will need to choose a compromise among the FAR and FRR values: the common applications try to hold lower possible these two indexes. To evaluate the global percentage of error of the system is used the EER (Equal Error Rate), defined as the percentage when the FAR and FRR are equal. With biometry must be defined a metric to establish the closeness of the comparison with a value of cut-off: only if the value associated to the biometric characteristic measured overcomes the cut-off value, then the system will recognize the user identity. Naturally, the system administrator, when establish a cut-off value, chooses a compromise (trade-off) among the probability of false acceptances (allowing the access the wrong person) and of false rejections (denying the access to the correct person). The (Figure 2) illustrates an example of some thresholds to establish the matching closeness of the biometric systems and the relative compromise among the indexes FAR and FRR.

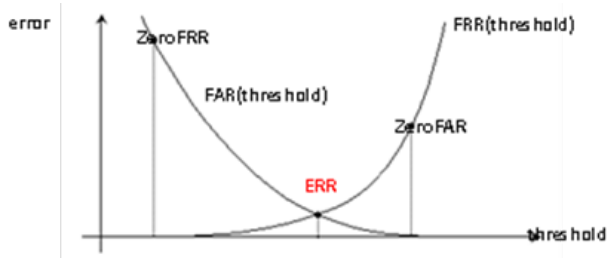

Figure 1 Typical course of FAR and FRR of a biometric system. The point where FAR is equal to FRR is EER point. Zero FAR is FRR value when FAR is zero; likewise Zero FRR is FAR value when FRR is zero.

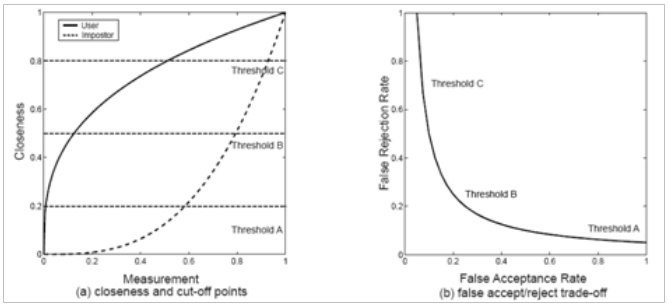

Figure 2 Matching closeness and thresholds (a) FAR versus FRR (b).

The (Figure 2A) shows two possible values distributions of closeness among user (continuous curve) and impostor (dashed curve). For any threshold chosen, sometimes will be true user refused and impostor accepted. Particularly, the false acceptances are to the right of the dashed curve and the false rejections are to the left of the continuous curve. In these systems to improve the accuracy, the area under the user distribution will increase and the area under the impostor curve will decrease. The (Figure 2B) illustrates the FAR versus the FRR, known as ROC (Receiver Operating Characteristic) varying the considered thresholds (A, B and C). A better accuracy of the biometric system reduces the space under this curve.

Biometric characteristics usability

The following Table 1 shows the more common human physiological and behavioral characteristics used to implement a biometric system.

These characteristics possess the following specific property[3]

I. **Universality:** Each person must have the characteristic used by the system.

II. **Distinctiveness:** The characteristic has to be distinguishable: two persons don't must be equal in terms of the same characteristic.

Citation: Conti V, Militello C, Vitabile S. Biometric authentication overview: a fingerprint recognition sensor description. *Int J Biosen Bioelectron.* 2017;2(1):26–31. DOI: 10.15406/ijbsbe.2017.02.00011

III. **Performance:** An optimum EER must be individualized.

IV. **Permanence:** The characteristics don't must change or modify during the human life.

V. **Acceptability:** The acquisition phase hasn't to be intrusive and the system has to be user-friendly.

VI. **Cost:** The system cost is always a problem that must be considered.

Table 1 Comparison between biometric technologies

Biometric technology	Universally	Distinctiveness	Permanence	Performance	Acceptability
Face geometry	High	Low	Medium	Low	High
Facial thermogram	High	Low	Medium	Low	High
Fingerprint	Medium	High	High	High	Medium
Hand geometry	Medium	Medium	Medium	Medium	Medium
Iris	High	High	High	High	Low
Retina	High	High	Medium	High	Low
Voice	Medium	Low	Low	Low	High
Calligraphy	Low	Low	Low	Low	High

Biometric techniques

In this section, the principal biometric technologies are illustrated. Each technology has advantages and disadvantages, in fact, don't exist an all-purpose correct technology for every system.[5] In the following (Figure 3), a classification of the most common biometric characteristics is given.

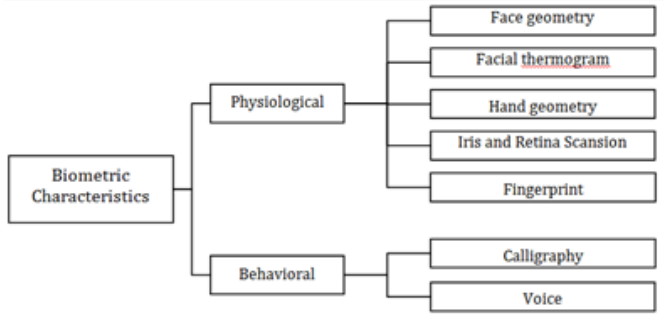

Figure 3 Classification of the most common biometrics characteristics.

Face geometry and facial thermo gram

The biometric systems using facial recognition[6,7] are based on the distance among facial attributes (i.e. the distance among the eyes) and on their shape (i.e. the mouth ampleness). In the system access phase a face image is acquired and provided to the system to compare it with the image stored in the database (Figure 4A). This technology has a good impact on the user, since it is less intrusive and it is not expensive. Facial geometry recognition approach is very sensitive to the variations in the illumination, to the different face positions and expressions.

The performances decrease when the dimension of the database increases (the twins are hardly distinguishable). The facial thermo gram[8] is based on the model of the blood vases and on the temperature of many face points (Figure 4B). Unfortunately facial thermo gram is sensitive to the emotional state and to the health state of the person.

Fingerprint recognition

The fingerprints are unique, don't change in the time and are different also in identical twins (Figure 5). Also this technology has some limits: excessively damp or dry skin can compromise the systems performances, sometimes fingerprints are not usable because of cuts or scars, besides they have an ugly impact on the user, for the association that is done between the figure of the criminal and the fingerprints. Such technology is the more common even if it is not easy to be implemented for big computational cost and request resources.[9,10]

Figure 4 Face geometry recognition (A) and facial thermogram recognition (B).

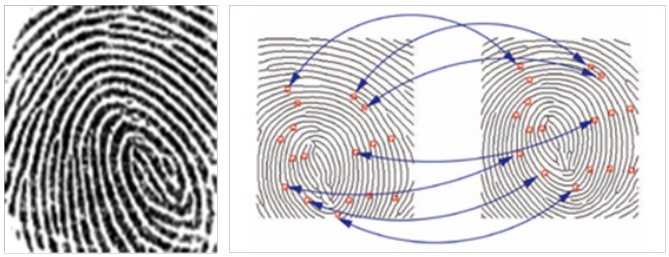

Figure 5 Fingerprint obtained by an optical scanner (A) and a matching between two fingerprint with micro-characteristics detected (B).

Hand geometry

The form and the dimensions of the hand can be used as distinctive characteristics.[11] The hand geometry recognition systems (Figure 6A) have many advantages respect the fingerprints: it requires less space to store the templates, the whole system is more convenient and meets small psychological resistance from humans. But also this technology has some defects: the people don't want to put the palm where many other have put theirs. The performances depend from the weather conditions or from the hand cleanness and the form of the hand is not invariant during the life. Finally, a real problem is the big dimension

Citation: Conti V, Militello C, Vitabile S. Biometric authentication overview: a fingerprint recognition sensor description. *Int J Biosen Bioelectron.* 2017;2(1):26–31. DOI: 10.15406/ijbsbe.2017.02.00011

of the hand sensor (Figure 6B), so this technology is not appropriate for some applications, how portable devices (cellular, pod and so on)

Figure 6 Hand geometry scansion (A) and hand geometry scanner (B).

Iris scansion

The iris scanning recognition[12,13] is based on the iris characteristics of the human eye (Figure 7B). After the DNA, the iris is the biometric characteristic more discriminating of the human body: also the identical twins have different iris. This technology uses particular video cameras for the scanning and is not necessary a contact between the eye of the subject and the biometric scanner (Figure 7A). The iris is less susceptible to damage respect to other parts of the body, the template asks only few byte for storage and the system works even if the person is carrying glasses.

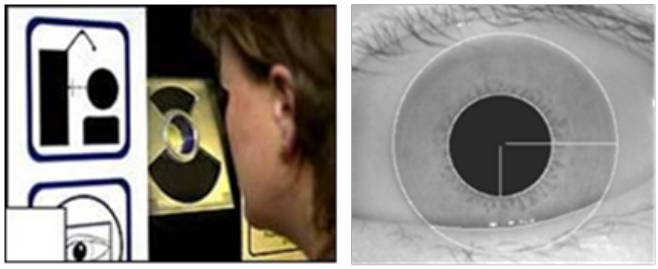

Figure 7 Scanner for iris acquisition (A) and iris segmentation (B).

Calligraphy recognition

This technique is based on the characteristic that every person has an unique style to write. A problem is that two writings of the same person are not never perfectly identical. This implicates a mediocrity reliability that brings this technology to be used only on small target of population. Two approaches exist for the calligraphy recognition: static and dynamic.[14] The dynamic method uses also acceleration, speed and pressure of the person that is writing for improving the recognition accuracy.

Retina scansion

The veins conformation under the retina surface of the eye is unique and therefore it is a characteristic usable for personal recognition.[15,16] The retina scanning is affected sending a beam of low intensity light inside the ocular bulb and storing the pattern constituted by the eye veins (Figure 8). The user has to be near the scanner and to focus a specific point with own eye: this type of system is less attractive. Besides the sensors are still rather expensive and the retina veins distribution changes during the human life.

Voice recognition

The voice recognition is considered the least accurate technology,[17] but it is preferred from the users and can provide the secure access to information through the telephone lines (Figure 9). The voice recognition can be text-dependent or text-independent: in the first case, the user says a predetermined sentence; in the second case (less accurate) the user simply says something.

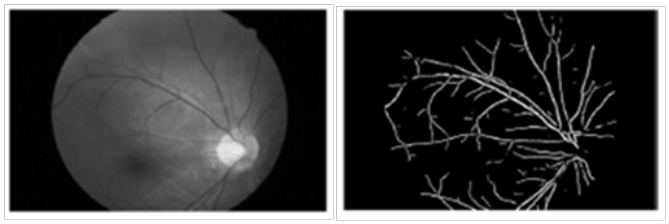

Figure 8 Human eye retinal blood vessel distribution (A) and retinal vessel tree segmented (B).

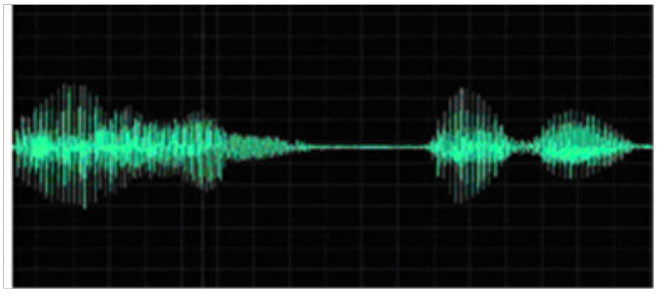

Figure 9 Voice signal representation.

The problem of this technology is that the user can realize a great variety of voice inflexions for environment variations or for stress. The environmental noises can strongly reduce the performances. The twins and the brothers are hardly distinguishable; also among different people the error percentages are high. This technology doesn't realize recognition on wide scale.

Choice of biometric technology

The biometric technologies guarantees the secure user recognition in different field, that mainly regard:[1,4,5]

i. **The physical accesses control:** it concerns those areas where it is important to recognize who enters and who go out (for example in the offices, hospitals, jails, etc...).

ii. **The logical accesses control:** it concerns the access through computer nets, cellular telephones, sets electronics to reserved data or services where security is important (e-banking, e-mail and so on).

The choice of biometric technology is usually done by the following factors:

I. The type of solution required

II. The environment where the biometric system will be used

III. The level of acceptance from the final user

IV. The requested security level.

The Table 2 shows some of the principal characteristics of the proposed technologies.

A fingerprint authentication sensor

In this section a fingerprints authentication system is described.[18–20]

Citation: Conti V, Militello C, Vitabile S. Biometric authentication overview: a fingerprint recognition sensor description. *Int J Biosen Bioelectron.* 2017;2(1):26–31. DOI: 10.15406/ijbsbe.2017.02.00011

This biometric sensor is composed of three modules: UIM, PM and AM (Figure 10).

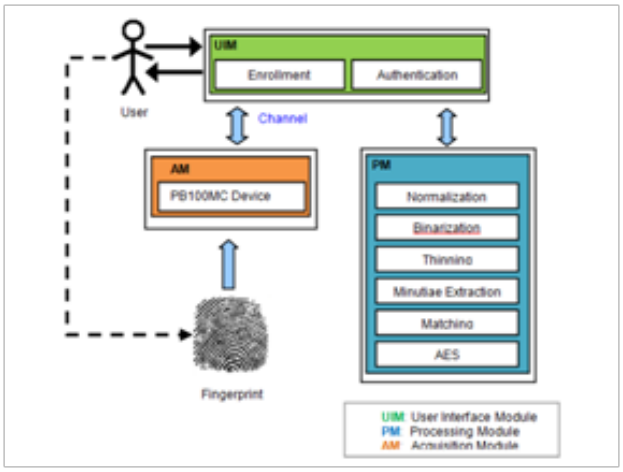

Figure 10 The three modules of the fingerprint recognition sensor.

UIM: user interface module

The UIM is a module expressly developed for providing the necessary interface to the user for access to the enrolment and authentication functionalities, provided by the biometric sensor. During the phase of enrolment, the followings steps can be individualized:

I. The user fingerprint is captured by the scanner PB100MC.

II. The image of the fingerprint is sent to the PM.

III. The minutiae are extracted and the biological template is created.

IV. The biological template is encrypted through the AES algorithm and stored in the system database.

Instead, in the phase authentication, it is possible to individualize the following steps:

I. The on-line fingerprint of the user is captured by the scanner;

II. The image of the on-line fingerprint and the ciphered biological template (acquired by the system in the enrolment phase) are sent to the PM;

III. The on-line image is processed by the PM and the relative minutiae are extracted and matched with the deciphered biological template present in the system database;

IV. If the result of the matching is positive (if the user is authenticated), it is granted the access to the user.

PM: processing module

The PM is a module that implements all the elaborations necessary to extract from fingerprints the biometric template. Are realised the followings six tasks: normalization, binarization, thinning, minutiae extraction, digital template encryption/decryption and matching.[21,22]

Table 2 Comparison between biometric technologies

Biometric Technology	Frr range (%)	Far range (%)	Cost	Template dimension (Bytes)	User acceptance
Face geometry	10÷20	0.001÷1	Medium	Few bytes	High
Hand geometry	1÷10	1	Medium	<10	Medium
Iris scansion	1÷10	~0	High	512	Low
Retina scansion	1	0.01	Very High		Low
Voice	10÷20	2÷5	Low	1500	High
Calligraphy	3÷10	1	Medium	1500	High
Fingerprint	3÷7	0.0001÷0.001	Medium	300÷1200	Medium

Table 3 FAR and FRR values considering a variable minimum percentage of minutiae matched and 2, 3 and 4 fingerprint to authenticate user

Sensor performance	Minutiae used for matching									
	85%		90%		93%		95%		97%	
Fingerprints number	FAR (%)	FRR (%)	FAR (%)	FRR (%)	FAR (%)	FRR (%)	FAR (%)	FRR (%)	FAR (%)	FRR (%)
2	6,35	3,13	2,99	5,21	1,68	7,29	1,07	8,33	0,98	11,46
3	3,93	8,33	1,71	14,58	1,12	17,71	0,78	22,92	0,71	26,04
4	2,16	25,00	0,99	32,29	0,87	40,63	0,60	46,88	0,41	52,08

AM: acquisition module

The AM manages the fingerprint scanner and the fingerprint capture. It is constituted by the device Precise Biometrics PB100MC and from the BSP (Biometric Service Provider) provided by the Bio APIs.[23,24] Inside the standard interface provided by the Bio APIs, the basic model of operation is the same, independently from the biometric technology used. First of all a user template must be created. The characteristics extracted by the samples, will go to constitute the template that will be memorized by the biometric system.

Recognitions analysis

The biometric system performance has been effected through the FAR and FRR percentages. An ideal authentication sensor would have FAR and FRR values equal to zero, instead, in a real system, users regularly recorded are refused by the system (false rejections) and users non-recorded are accepted (false acceptances). Thus the values of FAR and FRR are not zero. Naturally more lower are these values and best will be the recognition efficiency. For the evaluation of these index and for their optimal choice, different tests have been

Citation: Conti V, Militello C, Vitabile S. Biometric authentication overview: a fingerprint recognition sensor description. *Int J Biosen Bioelectron.* 2017;2(1):26–31. DOI: 10.15406/ijbsbe.2017.02.00011

effected on a set of 352 fingerprints of 88 users captured through the fingerprint scanned PB100MC.

Conclusion

Biometry allows the automatic user authentication sensor using his physiological or behavioral characteristics increasing the system security level. The biometric sensor constitutes a valid alternative respect the "conventional" authentication systems, based on traditional authentication methods (like password and PIN). The modern biometric sensors are less expensive and also more miniaturized and this allows an easier diffusion of biometric authentication systems. Besides the biometry is an effective strategy for the privacy protection. Finally, biometric sensors, in the future, will can be used in almost every transaction that needs secure personal authentication.

Acknowledgements

None.

Conflict of interest

The author declares no conflict of interest.

References

1. James Wayman. Biometric identification and the financial services industry. CA for the United States Department of Energy; 1991.
2. Paola Canali, Silvia Ciampoli, Giovanni D Ammassa, et al. Le Tecniche Biometriche. 2004
3. Militello C, Conti V, Vitabile V, et al. Embedded access points for trusted data and resources access in HPC systems. The Journal of Supercomputing. 2011;55(1):4–27.
4. Anil Jain, Lin Hong, Sharath Pankanti. Biometric identification. *Communications of the ACM*. 2000;43(2):90–98.
5. Anil Jain, Ruud Bolle, Sharath Pankanti. Biometrics. Personal identification in networked society, Springer; 2000.
6. Alex Pentland, Tanzeem Choudhury. Face recognition for smart environments. *IEEE computer*. 2000;33(2):50–55.
7. Chellappa R, Wilson C, Sirohey A. Human and machine recognition of faces: A survey. *Proceedings of the IEEE*. 1995;83(5):705–740.
8. Prokoski FK. Disguise detection and identification using infrared imagery. *Optics and Images in Law Enforcement II*. 1982; 0039:27–31.
9. Conti V, Vitello G, Sorbello F, et al. An advanced technique for user identification using partial fingerprint. *Intelligent and Software Intensive Systems*. 2013. p. 236–242.
10. Jain Anil. A multichannel approach to finger prints classification. *IEEE Transaction on Pattern Analysis and Machine Intelligence*. 1999;21(4):348–358.
11. Sidlauskas. 3D hand profile identification apparatus; 1998.
12. Michael Negin, Theodore Camus. An iris biometric system for public and personal use. *Journal Computer*. 2000;33(2):70–75.
13. Conti V, Milici G, Vitabile S, et al. An Novel Iris Recognition System based on Micro-Features. *IEEE workshop on Automatic Identification Advanced Technologies*. 2007. p. 253–258.
14. Nalwa V. Automatic on-line signature verification. *Proceedings of the IEEE*. 1997;85(2):213–239.
15. Hill RB. Apparatus and method for identifying individuals through their retinal vasculature patterns; 1978.
16. Bin Fang, Yuan Yan Tang. Elastic registration for retinal images based on reconstructed vascular trees. *IEEE Transactions on Biomedical Engineering*. 2006;53(6):1183–1187.
17. Furui S. Recent advances in speaker recognition. *Pattern Recognition Letters*. 1997;18(9):859–872.
18. Conti V, Vitabile S, Vitello G, et al. An embedded biometric sensor for ubiquitous authentication. AEIT Annual IEEE Conference; Italy: Springer; 2013. p. 1–6.
19. Vitello G, Sorbello F, Gentile A, et al. Design and implementation of an efficient fingerprint features extractor. *Digital System Design (DSD)*. 2014. p. 695–699.
20. Conti V, Militello C, Sorbello F, et al. Biometric sensors rapid prototyping on field-programmable gate arrays. *The Knowledge Engineering Review*. 2015;30(2):201–219.
21. Jain K, Hong L, Bolle R. On line fingerprint verification. *IEEE transactions on pattern analysis and machine intelligence*. 1997; 19(4):302–313.
22. Conti V, Militello C, Vitabile S, et al. Introducing pseudo-singularity points for efficient fingerprints classification and recognition. *Intelligent and Software Intensive Systems (CISIS)*. 2010. p. 368–375.
23. Catherine Tilton. An emerging biometric API industry standard. *Computer*. 2000;33(2):130–132.
24. 2001 Bio API Specification Version 1.1.