Editorial

BIOMETRICS is the discipline that measures human physiological traits (e.g., fingerprint, iris, face, retina, palmprint, hand shape, vein patterns, DNA, odor, color, electrocardiographical or electroencephalographical signals) and human behavioral traits (e.g., voice, facial expressions, gait, signature, handwriting, keystrokes on keyboards, body motion, posture).

These traits are significant to characterize the human beings from different perspectives. Some of these features (e.g., fingerprint, iris, face) are uniquely related to each individual, at least with an accuracy and a confidence degree depending on the specific trait considered. This uniqueness is very useful in security and forensics for person verification, identification, and recognition. Person verification certifies that an individual is who he/she claims to be by verifying his/her credentials with those stored. This can be used for access control, e.g., in border control with e-passports, e-commerce, e-banking, e-government, and access to restricted physical areas. Person identification systems searches for a specific individual in a database of persons by using his/her characteristic traits to retrieve the identity of the person, independently from what that individual declares, e.g., in border control and in suspect identification by police. A person recognition system tries to identify persons in the crowd, typically for security purposes. Other biometric features (e.g., facial expressions, gait, body motion) can be associated to psychological states, emotions, and movements of persons. These features can therefore be used to understand the attitude and the behavior of persons and the intentions behind their actions. Typical applications are in security and surveillance to detect and, possibly, prevent criminal actions.

A third group of biometric features (e.g., color, physiological signals, and odor) may be related to medical conditions of patients and, thus, be considered as symptoms of a disease by medical doctors. This may help in increasing the quantity of information collected by doctors in anamnesis, helping them to understand the patients' conditions and devise a better diagnosis and prognosis.

To increase reliability of biometric applications various studies were also successfully carried out by using multi-modal approaches (i.e., more than one biometric –of the same or of different types– to increase the total amount of features extracted from the data to characterize the individual or his/her conditions) and multi-paradigm strategies (i.e., more than one biometric data processing techniques to extract the characteristic features in different ways thus taking advantage of the most suited approaches for each operating condition and therefore reducing the influence of drawbacks of each specific technique).

Biometrics may be therefore incredibly helpful in designing and implementing advanced solutions for many applications which can benefit from qualitative and quantitative observations of human physiological or behavioral traits, as those mentioned above. For these reasons and thanks to the recent advances especially in signal and image processing, pattern analysis and recognition, and/or information processing architectures, nowadays, biometric research and applications are receiving continuously growing interest worldwide due to the criticality and the social impact of applications themselves.

Biometrics, although a narrow scientific and technological field, is highly interdisciplinary since it encompasses various aspects of different disciplines (e.g., physiology, biology, medicine, psychology, sociology, chemistry, physics, material sciences, computer science, computer engineering, electronics, system automation, telecommunications, and economics). Inter-disciplinary and synergetic interactions among various disciplines are key aspects of this area. To create a biometric system various issues need to be studied in an integrated way: from sensing to measurement procedures, from signal analysis and interpretation to quality assessment, from feature extraction to classification and analysis, from knowledge creation to extraction, from algorithms to data structure, from computational complexity to system performance, from system engineering to software engineering, and much more. Integration and cooperative combination are other key aspects of biometricsystems and applications.

Biometric security is yet another issue receiving more and more attention. Traditional biometric systems are vulnerable to various types of attacks, e.g., substitution attack, replay attack, and so on. The most important issue among them is the biometric template protection, since storage of raw templates in existing biometric systems can seriously compromise security. Recently many template protection related technologies have been developed, but this area of research continues to be an open problem.

Biometry privacy and social acceptance are also very critical aspects of using these technologies in daily-life applications. For example, if a password used for access control to a computer-based service is stolen, it can be replaced but damages are usually limited. Conversely, a biometry cannot be replaced and the thief will be able to fully impersonate the original owner forever: it is in fact absolutely impossible to change the biometry of the original owner since that physiological trait (e.g., fingerprint, iris, face) should be physically modified. On the other side, if the biometric feature is used for medical applications, its uncontrolled circulation makes the owner's medical conditions public, thus infringing his/her right to privacy. Citizens are therefore seriously concerned that their biometric traits may be stolen and misused, thus drastically reducing their confidence in adopting biometric-based solutions for advanced computer-based services.

Even though there is so much activity in biometrics theory and applications, a better understanding of these technologies, their opportunities, their limits, and the critical issues for their use in practical applications is still important, especially from

Digital Object Identifier 10.1109/JSYST.2009.2038953

an engineering point of view, to develop clear guidelines for conscious design and use of biometric-based systems.

This special issue therefore is a collection of original papers that address various aspects of the design, implementation and application of biometrics systems, by focusing on the system-level issues of biometric environments and applications, in order to deepen our knowledge on these issues which are considered fundamental for an effective and efficient use of these technologies in systems of real-world applications.

System design issues concerning hardware and software paradigms are the first aspects addressed by some papers in the special issue to ensure an appropriate design of the system architecture, its scalability, and its adaptability to changing environment and application needs. In "Biometric Sensor Management: Trade-offs in Time, Accuracy, and Energy" authors analyze the optimum choice of sensors for biometrics applications from a system perspective. In "Wireless Body Sensor Network with Adaptive Low Power Design for Biometrics and Healthcare Applications" the design of low-power sensors and components is studied to address needs of emerging wireless applications within complex monitoring and information systems. The use of multi-agent approaches to structure the system software are studied in "Analyzing the benefits of a novel multiagent approach in a multimodal biometrics identification task".

Effectiveness and efficiency of a biometric system are strongly related to specific characteristics of the techniques which are adopted to extract and process the biometric information. The quality of the biometric data is a challenging aspect for any system in order to achieve the desired accuracy in the envisioned application. In "A Fast Minutiae-based Fingerprint Recognition System" the authors focus on efficiency in extracting and processing biometrics features. In "Multiple Human Tracking and Identification with Wireless Distributed Pyroelectric Sensor Systems" the use of pyroelectric sensors is considered in a distributed environment for accurate thermal analysis.

Privacy of biometric information and traits is receiving an increasing attention since it is fundamental to ensure social acceptance of the biometric technologies. In "A Biometric Encryption System for the Self-Exclusion Scenario of Face Recognition" an approach is presented to protect the face trait, while in "Secure Computation for Biometric Data Security—Application to Speaker Verification" the voice is considered.

To have an actual use of biometric-based systems the presence and the interaction of humans must be carefully taken into account from the beginning of the system design. In "Biometrics Systems Include Users" a user-centered design of biometric-based systems is discussed. In "Leveraging Biometrics for User Authentication in Online Learning: A Systems Perspective" the use of biometrics for continuous non-intrusive identity verification is studied by considering e-learning systems as a specific application case.

More than 30 papers have been received for this special issue, but only nine papers have been accepted for publication since we aimed to create a high-quality issue which might become a major reference in the biometric systems arena. The review effort was tremendous: we like to thank thereforeing of these technologies, their opportunities, their limits, and the critical issues for their use in practical applications is still important, especially from an engineering point of view, to develop clear guidelines for conscious design and use of biometric-based systems.

We are sure that you will find this special issue interesting, informative, and enjoyable.

VINCENZO PIURI, *Guest Editor*
Università degli Studi di Milano
Milano, Italy
vincenzo.piuri@unimi.it

JIE TIAN, *Guest Editor*
Chinese Academy of Sciences
Beijing, China

EVANGELIA MICHELI-TZANAKOU, *Guest Editor*
Rutgers University
Piscataway, NJ 08854 USA