Harnessing the Power of Biosignals

Hugo Plácido da Silva and Ana Fred,
IT—Instituto de Telecomunicações and IST—Instituto Superior Técnico, Portugal

Biomedical signals such as electrocardiography waveforms can help address the long-standing problems of aliveness detection and continuous recognition in biometric systems.

As biometric technology finds use in a growing number of mainstream applications, from building access control to mobile device unlocking, it poses novel challenges for identity sciences researchers. Due to performance, user acceptability, and cost trade-offs, fingerprint, face, and iris recognition are the conventional choices for biometric products.[1] However, these modalities exhibit several inherent limitations that have been difficult to overcome: two such limitations are *aliveness detection* and *continuous recognition*.

Traditional biometric systems rely mostly on external anatomical traits that can be easily retrieved without user consent. Also, it's possible to physically extract some of these traits from an authorized user's body to gain illegitimate access to a system. For example, an attacker can fool a fingerprint scanner by using a gelatin finger mold from a latent fingerprint, or in some cases confound a face recognition system with a simple photograph. Aliveness detection ensures that a biometric signal is from a living source—ideally, its legitimate owner.

Biometric systems should also be able to continuously recognize a user to ensure that he or she is the same person initially authorized to access the system. However, fingerprint readers can become occluded by dirt, lotions, and oil from fingers, thereby necessitating repeated swipes, while face and iris recognition systems require precise orientation to the sensor and are heavily influenced by ambient light and changes in pose or facial expression.

To address these problems, identity sciences researchers are increasingly turning to biomedical signals such as cardiac activity, skin conductance, and temperature. These signals have several convenient properties—namely, they originate from a live source, are continuously available, and cannot be reproduced from latent impressions or remotely captured patterns. While low user acceptability and high costs once hindered research into biosignals, recent instrumentation advances are creating new opportunities to harness their power for biometric systems.

ALIVENESS DETECTION

Perhaps the best-known example of the perils of biometric recognition dates back to 2005, when a gang of car thieves in Malaysia severed the index finger of the owner of a high-end Mercedes S-class sedan to bypass its fingerprint recognition system.[2]

Despite the efforts of fingerprint scanner manufacturers to integrate additional countermeasures such as body temperature, sweat, or pulse sensing, attackers can still confound the system by using forged samples. In a 2006 episode of the popular science TV show *MythBusters* titled "Crimes and Myth-Demeanors 2," the team successfully bypassed a door-mounted fingerprint lock supposedly fitted with "liveliness-sensing" features using latex, ballistic gel, and even paper-printed reproductions of an enrolled fingerprint simply by licking the replica to simulate sweat.

Eight years later, a cloud still

Published by the IEEE Computer Society

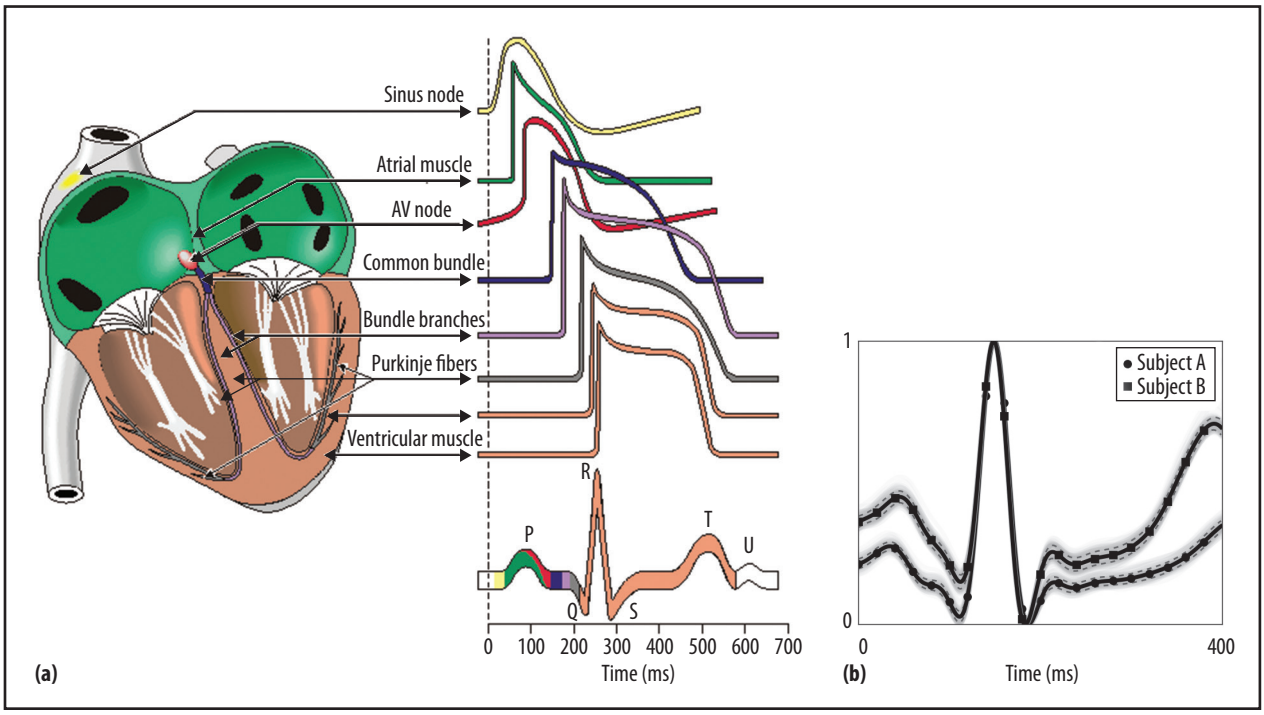

Figure 1. Electrocardiography (ECG) as the basis for biometric recognition. (a) ECG waveforms produced by each of the clusters of specialized cells found in the heart and their contribution to the prototypical heartbeat waveform. (Reprinted with permission from J. Malmivuo and R. Plonsey, *Bioelectromagnetism: Principles and Applications of Bioelectric and Biomagnetic Fields*, Oxford Univ. Press, 1995). (b) ECG waveforms with normalized amplitudes for two different users, illustrating intra- and interclass variability. The light gray lines show the individual heartbeat waveforms of each subject, the solid black line depicts the mean of all heartbeat waveforms belonging to a given subject, and the dashed black lines highlight the standard deviation.

hangs over fingerprint recognition technology. At a hospital in Brazil, a doctor was recently caught using silicon fingers to illegally clock six absentee colleagues into the hospital's time-card system.[3] And skepticism has surrounded Apple's Touch ID technology in the iPhone 5s in the wake of conflicting reports on its reliability.[4,5]

Fingerprint recognition isn't the only biometric technique in the spotlight; in 2011, facial recognition also had its share of unwelcome attention when the ability to bypass Android's face unlock feature with a photo became public.[6]

Aliveness detection remains an important and enduring problem, as evidenced by well-funded research initiatives such as the EU's Trusted Biometrics under Spoofing Attacks project (Tabula Rasa; www.tabularasa-euproject.org).

CONTINUOUS RECOGNITION

Once a biometric system—or any access control system, for that matter—recognizes a user's credentials as legitimate, it typically has no way of knowing whether the user remains the same throughout a session. Continuous recognition research focuses on developing methods capable of enabling continuous or near-continuous identity revalidation.

Existing solutions use either behavioral biometrics or some combination of biometric and nonbiometric technologies. An example of the latter is the Bloomberg Professional service, which provides account holders with a special keyboard containing a built-in fingerprint reader for user authentication as well as a portable, credit card–size fingerprint scanner called a B-UNIT that lets users access their account information from any location by using a PC or mobile device (www.bloomberg.com/professional/systems-support/hardware).

Behavioral biometric approaches, on the other hand, leverage a range of actions or mannerisms that tend to be unique to a given person and periodically executed. Perhaps the oldest and most studied technique involves keystroke dynamics, such as the amount of time the subject holds down a particular key or moves between keys. Watchful Software's TypeWATCH (www.watchfulsoftware.com/en/products/typewatch) is a recent example.

Other behavioral biometrics applications include gait analysis, which recognizes users by their walking or other mobility patterns,[7] and subject-specific mouse, touchpad, or touchscreen manipulation dynamics such as acceleration and speed.[8]

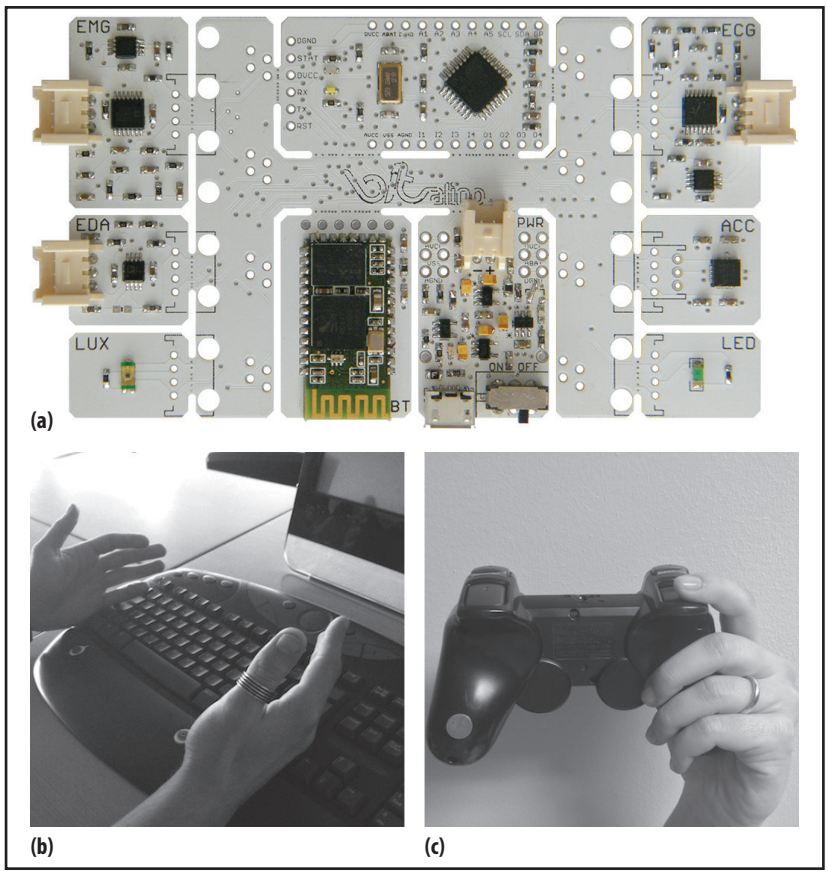

Figure 2. "Off-the-person" sensing. (a) BITalino hardware platform for physiological data acquisition. (b) Computer keyboard equipped with nongelled silver–silver chloride (Ag-AgCl) electrodes to continuously monitor ECG waveforms. (c) Off-the-person sensors seamlessly integrated into the handles of a videogame controller.

Continuous recognition is the focus of many ongoing research efforts including DARPA's Active Authentication program (www.darpa.mil/Our_Work/I2O/Programs/Active_Authentication.aspx), which launched in 2012 and is now in its second phase.

THE PROMISE OF BIOSIGNALS

Biosignals offer a promising solution to the limitations of current biometric systems, as they originate with a live source, enabling intrinsic aliveness detection, and are generally available in a continuous or near-continuous manner. In particular, electrocardiography (ECG) is at the forefront of biosignal-based biometric approaches.

As Figure 1a shows, the heart has an independent electrical system composed of several clusters of specialized cells, some of which—namely, the sinus node's pacemaker cells—are capable of self-stimulation. Each cell cluster uniquely contributes to the ECG waveform, as measured at the body surface. Considering that factors such as the size, shape, and position of the heart within the chest cavity vary among individuals, the waveform's P-QRS-TU segments likely reflect some of these intersubject variations, as Figure 1b shows.

Although more research is necessary, preliminary results indicate that ECG waveforms are measurably distinct across individuals and can serve as an effective modality for biometric verification even across several months. A recent experiment matching the ECG waveforms of 63 subjects collected at different time instants reported equal error rates below 2.01 percent for short-term data (minutes apart) and 9.68 percent for long-term data (months apart).[9]

The high costs and usability problems associated with physiological sensors—including intrusiveness, bulkiness, and nonportability—have been major barriers to a more extensive use of ECG waveforms and other biosignals in the identity sciences community. However, recent improvements in sensor technologies are opening new opportunities for biosignal-based approaches, especially through the recent shift toward "off-the-person" sensing[10] and the advent of low-cost biosignal acquisition hardware such as BITalino (www.bitalino.com). Figure 2 shows a BITalino-based off-the-person sensing system, integrated into a keyboard and videogame controller, which captures ECG waveforms from the user's fingers via nongelled silver–silver chloride (Ag-AgCl) electrodes.

Biosignals such as ECG waveforms have great potential to help address the long-standing problems of aliveness detection and continuous recognition in biometric systems. The availability of inexpensive, easy-to-deploy physiological sensors and hardware platforms now makes it possible to seamlessly and cost-effectively integrate biosignal authentication with traditional fingerprint, face, and iris recognition, providing an additional security layer.

References

1. K. Ricanek Jr., "Dissecting the Human Identity," *Computer*, vol. 44, no. 1, 2011, pp. 96–97.
2. J. Kent, "Malaysia Car Thieves Steal Finger," *BBC News*, 31 Mar.

2005; http://news.bbc.co.uk/2/hi/asia-pacific/4396831.stm.
3. L. Hutchinson, "Brazilian Docs Fool Biometric Scanners with Bag Full of Fake Fingers," *Ars Technica*, 13 Mar. 2013; http://arstechnica.com/tech-policy/2013/03/brazilian-docs-fool-biometric-scanners-with-bag-full-of-fake-fingers.
4. "Chaos Computer Club Breaks Apple Touch ID," blog, 21 Sept. 2013; www.ccc.de/en/updates/2013/ccc-breaks-apple-touchid.
5. A. Strange, "No, A Severed Finger Will Not Be Able to Access a Stolen iPhone 5s," *Mashable*, 15 Sept. 2013; http://mashable.com/2013/09/15/severed-finger-iphone-5s.
6. G. Kumparak, "Yes, Android's New Face Unlock Feature Can Be Fooled with a Photo," *TechCrunch*, 11 Nov. 2011; http://techcrunch.com/2011/11/11/android-facial-unlock-photo.
7. D. Matovski et al., "The Effect of Time on Gait Recognition Performance," *IEEE Trans. Information Forensics and Security*, vol. 7, no. 2, 2012; doi:10.1109/TIFS.2011.2176118.
8. H. Gamboa and A. Fred, "A Behavioural Biometric System Based on Human Computer Interaction," *Proc. SPIE: Biometric Technology for Human Identification*, vol. 5404, 2004, pp. 381–392.
9. H.P. da Silva et al., "Finger ECG Signal for User Authentication: Usability and Performance," *Proc. IEEE 6th Int'l Conf. Biometrics: Theory, Applications and Systems* (BTAS 13), 2013; doi:10.1109/BTAS.2013.6712689.
10. H.P. da Silva et al., "Off-the-Person Electrocardiography," *Proc. 1st Int'l Congress on Cardiovascular Technologies* (Cardiotechnix 13), 2013, pp. 99–106.

Hugo Plácido da Silva *is a researcher at the IT—Instituto de Telecomunicações, and a PhD student at the IST—Instituto Superior Técnico, Portugal. Contact him at hugo.silva@lx.it.pt.*

Ana Fred *is a researcher at the IT—Instituto de Telecomunicações, and an associate professor at the IST—Instituto Superior Técnico, Portugal. Contact her at afred@lx.it.pt.*

Editor: Karl Ricanek Jr., director of the Face Aging Group at the University of North Carolina Wilmington; ricanekk@uncw.edu