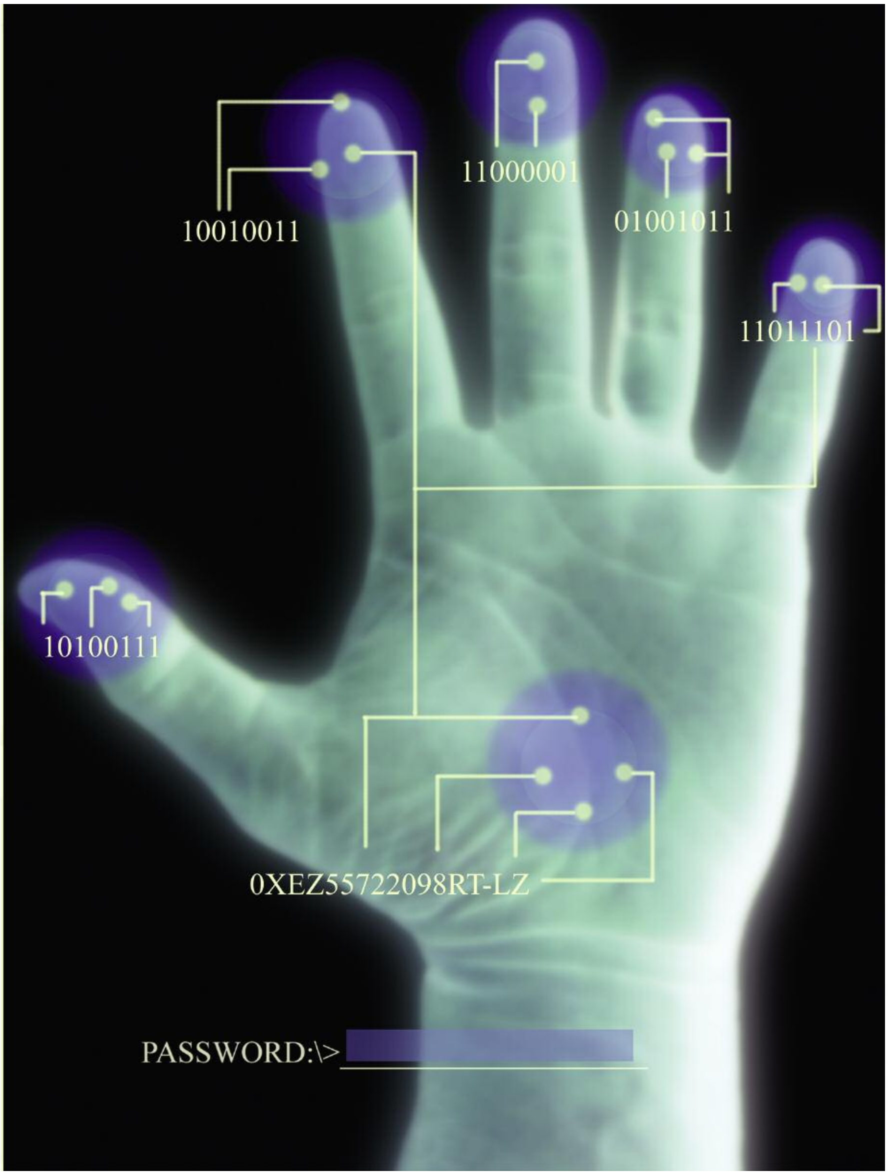
Biometrics as an Assistive Technology

Judith Katz

With a demographic shift that finds the majority of the world's population consisting of adults over the age of 65 and fewer younger people available to care for the aging, the need for innovations that support and foster greater independence was a prime topic at the 2007 International Association of Homes and Services for the Aging Conference.

Projections suggest that by 2026, the population of Americans ages 65 and older will double to 71.5 million. Between 2007 and 2015, the number of Americans aged 85 and older is expected to increase by 40%. And, among people turning 65 today, 69% will need some form of long-term care (LTC), whether in the community or in a residential care facility.

Innovative ideas and technologies are crucial for meeting the complex needs of this ever-growing group of aging adults. Among systems that can aid in monitoring the activities and habits of older adults is biometric recognition technology. Since their introduction, biometric devices have become a popular and preferred method in all types of security applications; from safeguarding borders and computer networks to managing facility access and time and attendance.



The term *biometric* is derived from the Greek words *bios* for life and *metron* for measure and has become an increasingly popular method of identity confirmation. In integration with computer technology, it is the digitization of unique physical traits such as fingerprints, voiceprints, retinal patterns, and other measurable physiological or behavioral characteristics. It is the one form of identification a user cannot leave home without and as such, provides aging individuals with an unmatched level of simplicity and convenience. Not surprisingly, it is widely used in applications that enhance functionality and help safeguard the welfare of assisted living (AL) residents and workers.

Biometrics delivers a noninvasive method for automatically identifying or verifying the identity of an individual based on physiological or behavioral characteristics. Increasingly over the past 2 decades, such authentication is accomplished by using computer technology to match patterns of live individuals in real-time against enrolled records. Examples include products that recognize faces, hands, fingers, signatures, irises, voices, fingerprints, and dermis patterns. Simply put, biometrics is the technology that in essence makes you—the user—the password.

Alternative systems that compete with biometrics as the credential used with data-capture systems are available, but because they permit sharing or duplication, cannot offer the same level of security.

Swipe-card systems. These plastic cards have information embedded on the card via a magnetic stripe or barcode. Each code corresponds with a particular individual and serves to identify that person. When these cards are swiped through a scanning device, the codes are read and an individual is identified.

Direct-entry systems. These digital key-code systems require users to enter personal identification numbers. Assigned alpha-numeric codes, commonly known as *PINs* (personal identification numbers), identify the person associated with that number. They can be used with or without cards. Individuals may either key their PIN numbers into a terminal or just insert their cards into a scanner to read the coded data.

Proximity device systems. These systems use radio frequency identification (RFID) technology. A microchip is embedded in an accessory such as a card, badge, or key fob, which transmits unique information to a reader. Proximity systems come in two types that either require contact or are contactless. In a contactless system, the chip has an antenna that enables the accessory to be waved at the reader from a distance. Contact systems function in the same way as their swipe-card counterparts, requiring direct contact between the chip and the reading device.

Biometrics is the one form of identification a user cannot leave home without, providing aging individuals an unmatched level of convenience.

In contrast, a biometric recognition system is charged with comparing new input of a fingerprint, iris, handwriting, voice pattern or some other identification to an original sample to determine a match. When a match is achieved, the person's identity is affirmed. When rejected, the input is assumed to be a forgery.

The objective of every biometric system is to resolve this pattern recognition problem with the goal being differentiation between originals and forgeries. In a typical information technology (IT) biometric system, a person is "enrolled" by providing a sample of his or her unique trait. This unique trait is then processed by software that converts it into a digital format (a file of a numerical representation) and enters it into the database for future comparisons to new input, which will then be analyzed to determine a match. This comparison occurs each time the individual logs in with the system. Ideally, the features from each recurring log-in will match 100% with the original sample. When a match does not occur, the system either refuses or red flags the log-in, notifying administrators of the discrepancy.

Systems that apply the technology do so in one of two distinct ways: identification or verification. With identification, the task is to determine *who* a person is by finding his or her match with a database of digitized biometric records. In cases in which the database contains hundreds or even thousands of records, the search can take substantial time and processing power. The second approach, verification, is the comparison of new input with the original sample.

Performance of a biometric measure is commonly referred to in terms of a false accept rate (FAR), a false nonmatch or reject rate (FRR), or a failure to enroll rate (FTE or FER). Yet, one of the most common measures of real-world biometric systems is the rate at which the setting equally accepts and rejects errors. The lower the equal error rate (EER; also known as the *crossover error rate [CER]*), the more accurate the system is considered. And overall, biometric systems are regarded as providing a very high degree of certainty and therefore a very high rate of reliability.

The second part of *Biometrics as an Assistive Technology* (see the September/October 2007 issue of *ALC*) will compare today's leading data capture technologies, detail how they work, explore their strengths and weaknesses, provide a list of criteria to aid the AL administrator evaluate and select the system best suited to the needs of the facility, and present the experience of a facility utilizing biometrics to manage its business challenges. ALC

Judith Katz is the CEO of Count Me In, LLC (www.countmeinllc.com), a developer of fingerprint-based software solutions.