Biometric Authentication: Privacy Protection or Invasion?

Save to myBoK

by Daniel J. Pothen, MS, RHIA, and Bambang Parmanto, PhD

Imagine using your fingerprint to access patient information maintained in your health system's data warehouse, or positioning your face in front of a device used to scan users' facial features to access your facility's clinical information system. But there's no need to imagine this anymore-biometric authentication devices have matured and become more affordable. And with increased government focus on ensuring the privacy and confidentiality of patient information and HIPAA's mandate of creating a universal patient identifier, you may be seeing these biometric authentication systems instituted in a healthcare facility near you.

Identification Through Authentication

What is biometric authentication? Put simply, it is the use of an electronic device to identify or verify a person using his or her unique identifying characteristics or traits. Your fingerprints, retinas, voice, and facial features are all unique attributes that can be used to authenticate your identity through the use of a biometric authentication device.

These devices differ from other authentication mechanisms, such as passwords, user IDs, or personal identification numbers, because biometric devices exploit a person's distinct physical characteristics by using them as the key to gain access to restricted systems, such as your facility's network. Unique identification or verification without the fear of replication or duplication for access to confidential health information is critical, and biometric authentication devices may be a formidable opponent to anyone attempting to gain unauthorized access to health record information.

However, biometrics do pose a risk: because they are used to verify unique personal information and are so reliable as personal identifiers, individuals may feel their privacy is threatened or compromised through the use of a biometric authentication device.[1]

Various types of biometric methodologies are used today. Fingerprint matching is the oldest methodology, while facial recognition has the most promising potential for authentication technology. Other popular biometric methodologies include iris and retinal scanning and hand geometry. Below, we'll take a closer look at each of these technologies.

Fingerprint Verification

Among all the biometric methodologies, fingerprint verification is the oldest and most popular. Because everyone is known to have unique, immutable fingerprints, fingerprinting has become the international standard for traditional identity verification among police forces. A fingerprint is made of a series of ridges and furrows on the surface of the finger. The uniqueness of a fingerprint can be determined by the pattern of ridges and furrows as well as the minutiae points (contours or points unique to each fingerprint).

There are a variety of approaches to fingerprint verification, but in general they can be placed into two categories: minutiae and pattern matching. Minutiae-based techniques try to emulate the traditional police method of finding minutiae points and then mapping their relative placement on the finger. Pattern matching takes a global view of the fingerprint and compares the overall pattern of the fingerprint images.

Retinal Scanning

In this methodology, the unique patterns of the retina are scanned by a low-intensity light source via an optical coupler. This established technique involves analysis of the layer of blood vessels at the back of the eye. Although quite accurate, this methodology requires the user to look into a receptacle and focus on a given point. For users with eye glasses or concerns

about contact with the reading device, it is not particularly convenient. For these reasons, retinal scanning has a few user acceptance problems.2

Iris Scanning

Iris scanning can overcome some of the difficulties of retinal scanning. First, it is less intrusive because it uses a fairly conventional camera element and requires no close contact between the user and the reader. Further, it has also been demonstrated to work with glasses in place. The system's ease of use and integration are drawbacks, but improvements are expected.

Speaker Verification

Speaker verification biometrics take advantage of the speaker-specific characteristics of speech, which are due to differences in physiological and behavioral aspects of the speech production system in humans. The new generation of voice verification devices use advanced analysis that makes utterances spoken by the same person but at different times result in similar sequence patterns that can be matched to the voice of the person.

Hand Geometry

As the name suggests, this approach uses the geometric shape of the hand to authenticate a user's identity. Unlike fingerprints, the human hand isn't unique. However, by combining various individual features, it is possible to attain robust verification. One of the most established methodologies, hand geometry offers a good balance of performance characteristics and is relatively easy to use.

Facial Recognition

Face recognition involves the analysis of the user's facial characteristics. It requires a digital camera to develop a facial image of the user for authentication. This technique has attracted considerable interest due to the promise of unobtrusively detecting and verifying the identity of an individual. Unfortunately, facial recognition is not as easy as matching two static images. To date, facial recognition systems have had limited success in practical applications. However, progress continues to be made in this area and if technical obstacles can be overcome, we may eventually see facial recognition emerge as a primary biometric methodology.

Multiple Biometrics

Identification based on multiple biometrics represents an emerging trend. This is especially appealing in situations where strict performance measures must be met. A biometric system relying only on a single biometric technique is often unable to meet the desired performance requirements. For example, face recognition is fast but not reliable while fingerprint verification is reliable but inefficient. Combining the two techniques can meet the response time and accuracy requirements.

HIPAA Meets Biometrics

In a presentation on HIPAA security and supporting technologies at the 2001 Annual HIMSS Conference, Tom Hanks, a consultant with Beacon Partners, explained that HIPAA requires a mechanism to ensure the authentication of the user and restrict the user to systems he or she is authorized to access.3 With that in mind, some facilities may entertain the idea of using biometric authentication devices to comply with this requirement. Hanks added that biometric devices "can increase the authentication strength and provide more assurance that only authorized users have access to the information."4

While biometrics may have an edge over other authentication devices, the concern remains that biometrics hold the key to distinctly identifying individuals. This is highly sensitive information and safeguards need to be in place to protect it. Would you be willing to use a biometric authentication device knowing that your unique identifiable information is stored and maintained by your facility or employer?

Biometrics as Unique Patient Identifiers

Employing biometrics as a unique patient identifier may be an option in the future, and the NCVHS has compared biometric identification methods against ASTM's conceptual characteristics of a unique patient identifier as being accessible, identifiable, assignable, verifiable, mergeable, and splittable.5 In a 1997 report, the NCVHS discusses the benefits and weaknesses of various biometric devices. Further, the report acknowledges that one of the major barriers to implementation of biometrics as a unique patient ID are the personal characteristics involved in authentication and that it may threaten individual privacy.

How Biometrics Affect HIM

HIM professionals at all levels must be aware of the existence of biometric devices as an authentication tool. With the recently passed HIPAA privacy regulations, healthcare organizations will be looking for new methods to protect access to health information and may wish to consider biometric authentication as an option for user authentication management. The chief privacy officer of your organization will likely be involved in selection of authentication tools used by staff for accessing information systems. As a result, a complete understanding of how biometrics work and the potential privacy concerns of individuals must be addressed by the privacy officer before implementation of such a system occurs.

Notes

1. Moskowitz, R. "Are Biometrics Too Good?" Network Computing 10, no. 2 (1999). Available at www.networkcomputing.com/1002/1002colmoskowitz.html.
2. Liu, S. and M. Silverman. "A Practical Guide to Biometric Security Technology." IEEE Computer Society, IT Pro 3, no. 1 (2001).
3. Hanks, Thomas L. 2001. "HIPAA Security: Supporting Technologies." Presented at 2001 Annual HIMSS Conference and Exhibition, February 4-8, New Orleans, LA.
4. Ibid.
5. Appavu, Soloman. "Unique Patient Identifiers Based on Biometrics." National Committee on Vital and Health Statistics. Available at http://ncvhs.hhs.gov/app7-6.htm.

Daniel Pothen (dpothen@deloitte.com) is a consultant in the integrated health group of Deloitte & Touche, LLP, in Los Angeles. Bambang Parmanto (parmanto+@pitt.edu) is assistant professor in the department of health information management at the University of Pittsburgh.

Article citation:
Pothen, Daniel J. and Bambang Parmanto. "Biometric Authentication: Privacy Protection or Invasion." *Journal of AHIMA* 72, no.7 (2001): 24-26.
