Biometrics: The Password You'll Never Forget

R.D. McDowall, McDowall Consulting, Bromley, Kent, UK.

In the last "Pharmaceutical File" (1) we discussed electronic signatures and logical security within the context of the Electronic Records and Electronic Signatures Final Rule (21 CFR 11) (2). Electronic signatures consist of a unique combination of user identity and password, and we discussed some of the issues surrounding the security of passwords and the access control needed for an application or system. This was covered under the umbrella term of logical security.

In this column, we'll be looking at logical security from a different perspective. Logical security can consist of one of three elements. Going from the lowest to the highest levels of security these include:

- *Something that you have*: Typically this can be an identity or security badge with a photograph and either magnetic or barcode information on it. Well, we know that's about as useful as using a sieve for holding water: I've left my card at home can I borrow yours? Of course, that never happens in your organization, does it?
- *Something that you know*: Typically this is a password used to access a computer. This is a relatively inexpensive and widespread means of ensuring computer security. We discussed the advantages and disadvantages of passwords previously (1) including the password paradox in which passwords that are easily remembered are the easiest to compromise but the secure computer-generated ones are more easily forgotten. One area within this type of security not explored last time was a digital signature that uses encryption to ensure data authenticity and data integrity. We'll be looking at this area in the next "Pharmaceutical File."
- *Something that you do or something that you are*: This uses a biological feature or characteristic of an individual that uniquely identifies them from anyone else. This is termed biometrics and is the subject of this column.

Combining two or more of these elements above can increase the security of an application. For example; the INSPASS system for entry of aliens into the USA (at least the ones arriving from overseas rather than from outer space) uses a combination of an ID card combined with a biometric hand-scanning device to determine the identity of an individual. This means that a relatively low-cost biometric device can be implemented with an additional identification device to produce a higher degree of security than can be obtained by using each one individually. Therefore, the identity of a person is confirmed by the unique combination of the correct card with the correct hand.

Biometrics Defined

The subject of this column is biometrics, which is defined as "…a method of verifying an individual's identity based on measurement of the individual's physical feature(s) or repeatable action(s) where those features and/or actions are both unique to that individual and measurable" (2).

To help decipher what this means, we'll be discussing biometrics in this column and how they relate to 21 CFR 11. These methods of identification are intended for open systems (1, 2) but as e-commerce becomes more widespread, better security is required and as the biometric devices become more cost-effective and reliable they will probably be used for closed systems as well. The advantage of using biometrics is that it will eliminate many of the problems caused by passwords and the procedures to administer them.

Biometrics refers to a unique, measurable characteristic of a human being that can be either a physical or behavioural characteristic. The rationale of using a biometric is that we will be using a particular part of our human make-up that makes each of us unique. The problem is to select a characteristic that can be captured, interpreted mathematically and used to identify or verify each of us using a computer.

User Identification or Verification?

It is important to understand how we are using biometrics in our computer systems for whatever reason. This boils down to the question of are we using biometrics to identify an individual from everyone else or to verify that someone is who they say they are. There is a world of difference between these two and you'll need to be aware of both.

Identification asks the question "Who is this?" (or "Are my fingerprints on the brick that was thrown through the jeweller's window?"). This requires the system to select one record from many; searching through the records of all individuals and listing only those patterns that match the scanned biometric. It establishes whether more than one biometric record exists — thus denying an individual that is attempting to pass him or herself off with more than one identity. This will take time and is not going to work with a real-time system where a user wants to gain access to a system or sign records. You'll not want to wait two hours to log on to your computer while the reference database is being searched and compared, will you? Please do not answer this question. It is rhetorical!

Verification asks the question "Is this person who he/she claims to be?" and is used to confirm, for example, that someone using an ID card is its true owner. This is the same way as the INSPASS method, described earlier, is used. It is a one-to-one process (comparing one template with the one sample, where the biometric system is seeking to authenticate an individual's claimed identity) and is faster, permitting real-time use.

Knowing these two fundamental aims, the key question is how are we going to use biometrics in the chromatography

laboratory? Why should we bother to answer this question when the Food and Drug Administration (FDA) has already answered it for us? Read 21 CFR 11 and discover the answer under §11.100(b), which states that before an organization establishes, assigns, certifies, or otherwise sanctions an individual's electronic signature, or any element of such electronic signature, the organization shall verify the identity of the individual.

Therefore, you'll be using biometrics for verifying the identity of users. This will reduce the complexity of the system and the computing requirements.

Types of Biometric System

Each biometric product either under development or commercially available in the market can be categorized as falling into one of the biometric technology areas. The main biometric technologies are

- face recognition
- finger scanning
- finger geometry
- hand geometry
- iris recognition
- palm prints
- retina patterns
- signature verification
- voice recognition
- other biometrics (i.e., vein pattern, typing rhythm).

It sounds very good and the principles of the main biometric methods are outlined in Table 1.

The Biometric Procedure

All biometric systems essentially operate in a similar way in a four-stage process that is automated and computerized, as shown in Figure 1.

Capture: A physical or behavioural sample is captured by the system during enrolment. First, a biometric system captures a sample of the biometric characteristic (fingerprint, voice etc.).

Extraction: Unique data are extracted from the sample and a template is created. Unique features are then extracted by the system and converted into a mathematical code (biometric data). This sample is then stored as the biometric template for that person.

Comparison: The template is then compared with a new sample. The biometric data are then stored as the biometric template (also known as the template or reference template) for that person.

Match/non-match: The system then decides whether the features extracted from the new sample are a match or a non-match with the template. When identity needs checking, the person interacts with the biometric system for a

Table 1: Main Types of Biometrics.

Biometric input	Main features
Face recognition	• Principle: analysis of the unique shape, pattern and positioning of facial features. • Highly complex technology and largely software based. • There are essentially two methods of capture: using video or thermal imaging. The latter is more expensive because of the high cost of infrared cameras. • Primary advantage is that the biometric system is able to operate "hands-free" and a user's identity is confirmed by simply staring at the screen. • Continuous monitoring of the user. • Access to sensitive information can be disabled when the user moves out of the camera's field of vision. Verification is then performed when the user returns to work at the desktop.
Finger scanning (verification)	• Principle: analysis of minutia points (finger image ridge endings, bifurcations or branches made by ridges). • One of the most commercially successful biometric technologies. • Important for applications where it is necessary to verify the identity of those who gain access.
Hand geometry	• Principle: captures a three-dimensional image using a camera when a hand is placed on a hand reader. • Very resilient and capable of handling a large throughput of end-users.
Finger geometry	• Principle: using similar principles to hand geometry, a three-dimensional image of the finger is captured using a camera. • Proven in the area of physical access control. • Very durable and copes well with external conditions.
Iris recognition	• Principle: analysis of the iris of the eye, which is the coloured ring of tissue that surrounds the pupil of the eye. • This is a highly mature technology with a proven track record in a number of application areas.
Palm	• Principle: similarities with the techniques adopted by finger scanning using minutiae found in the palm.
Retina	• Principle: The retina is the layer of blood vessels situated at the back of the eye. The scanning technique to capture data from the retina is often thought to be the most inconvenient for end-users. An end-user must focus on a green dot and when this has been performed, the system uses a harmless beam of light to capture the unique retina characteristics. • Considered the most accurate of all biometrics.
Signature	• Principle: the movement of the pen during the signing process rather than the static image of the signature. • Many aspects of the signature in motion can be studied, such as pen pressure, the sound the pen makes against paper or the angle of the pen that makes this a behavioural biometric. • We learn to sign our name, and our signature is unique because of this learning process. The speed, velocity and pressure of the signature remain relatively consistent. • Signature systems can rely either on a special tablet or a special pen.
Voice recognition	• Principle: analysis of the unique characteristics of voice as a merger of physical and behavioural characteristics (physical dimensions of the voice box and the sounds adopted as speech is learnt). • Very little hardware is required (e.g., a microphone on a standard PC with software to analyse the unique characteristics). • Ideally suited to telephone-based applications.

second time, a new biometric sample is taken and compared with the template. If the template and the new sample match, the person's identity is confirmed.

How Does It Work? Putting Your Finger on It!

We've seen the principles outlined above. I'll explain how fingerprint recognition, a common method of biometrics, works. The principles outlined here are applicable to all other methods of biometrics, although the features that are mathematically represented will vary. We'll just take a single pass through the process and assume that the reference templates have already been identified. The overview of the process is shown in Figure 2.

The principles that fingerprint scanning are based upon are as follows:

- No two fingerprints from different fingers have the same ridge pattern
- This pattern does not change throughout life.

Other biometric techniques will capture other unique characteristics as described in Table 1.

Fingerprints have been used for a number of years for identification and crime prevention or detection and have a long history of use, and you'll be familiar with the approach — more through films than personal experience, I hope.

Moreover, Compaq has offered a biometric fingerprint scanner as standard with some models of workstation for corporate networks since the middle of 1998. For these reasons, I've chosen fingerprinting to describe the biometric process in detail for verification of identity as described below and in Figure 1.

Capture: The finger to be scanned (usually a left or right index finger) is placed upon a scanning device; the user may need to activate a log-on screen first or be in a program where an electronic record is to be signed. The scanner is usually a passive infrared device that is connected to a workstation that captures the fingerprint, and the digital scan is fed into the next stage of the process. The scanner plate needs to be kept free of dirt and smudges that could interfere with the scanning of a finger.

Extraction: The image of the fingerprint scan needs to be enhanced, as a good image increases the certainty of verifying an individual. The problem is that fingers tend to be at the business end of many tasks and they become dirty, cut, wet and worn (dipping fingers into sulfuric acid should be an interesting validation experiment, as would cutting your index finger. Note the emphasis on YOUR and not mine here), and the image enhancement is necessary to help define the ridges and valleys.

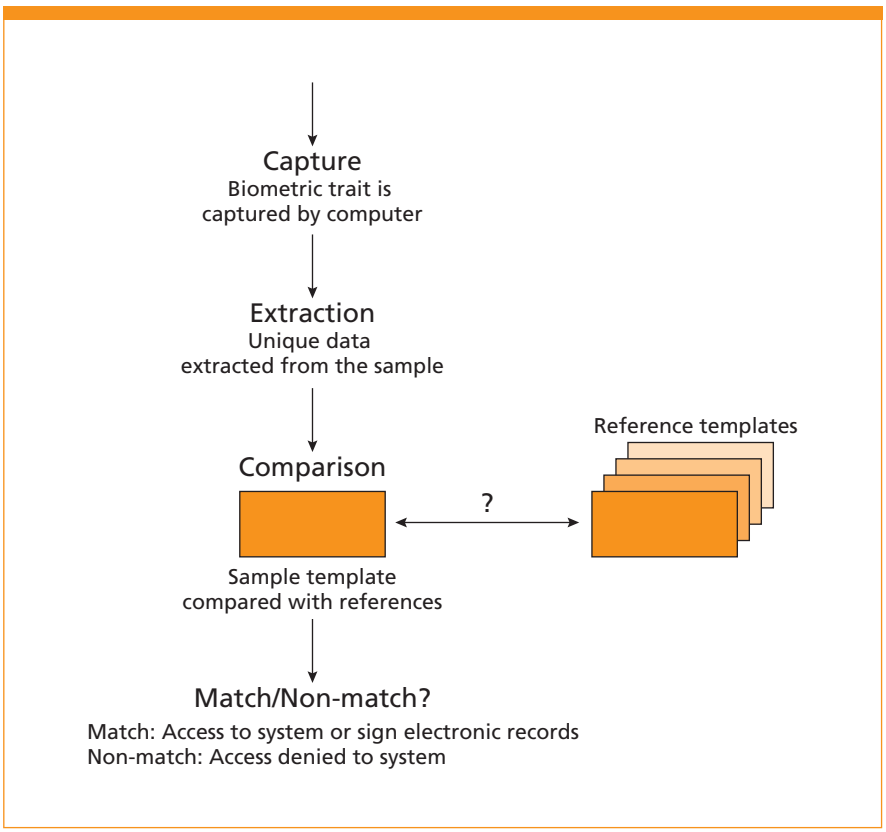

Figure 1: *Biometric procedure.*

The features of the fingerprint are examined by pattern recognition software. A small discourse on fingerprints is required to explain this approach. Fingerprints consist of unique patterns of ridges (raised areas) and valleys (spaces between the ridges); comparison is usually based on the ridges for identification. The main method of biometric identification uses minutiae. A minutia is either where a ridge ends (ending minutia) or where a ridge branches (bifurcation minutia), as shown in Figure 2.

The scanned image is thinned to a single pixel to help minutia detection: endings are found at the end of lines and bifurcations found at the junction of three lines. Each minutia is assigned information such as type, location and direction. The minutiae are usually linked together into a graph and this forms the template for the identification.

Comparison: The extracted information is compared with the reference template to see whether the two are similar to verify an individual's identity. The system is looking for similarities, as exact matches are unlikely for reasons such as noise in the scanning system. Moreover, as skin is elastic the distances will vary between minutiae to some extent (consider whether the laboratory is cold or hot for instance if you have just been changing the "O" rings on a GC column or taken a sample from a freezer).

Match/non-match: There is usually a threshold value for the match, and if the score is above this then the identity is verified. This will be reported and access to the system will be allowed or denied according to the results.

Good in Principle, But…

There is always a 'but' somewhere and for biometrics it's the fact that biometric systems are not 100% accurate 100% of the time. Humans are inconsistent: both our physical and behavioural characteristics can change over time and a finger can be cut (any volunteers for that validation study by the way?).

So any biometric system needs to allow for these subtle changes and a threshold value is set for the comparison. Comparison between the reference and new sample must exceed the system's threshold before a match is considered. In other words, if the new biometric sample is considered by the system to be sufficiently similar to the template, the system will

determine that the two do in fact match. This approach gives the system a degree of flexibility over a traditional password that must match exactly for a user to gain access. However, this brings an element of performance assessment with biometrics systems.

False Rejection and False Acceptance

The biometrics industry has used two performance measurements to rank a biometric system's level of matching accuracy. These focus on a system's ability to allow access to unauthorized users and deny access to those who are authorized.

- False rejection rate (FRR) is concerned with the number of instances an authorized individual is falsely rejected by the system.
- False acceptance rate (FAR) refers to the number of instances an unauthorized individual is falsely accepted by the system.

Obviously, these two measures should be as low as possible to avoid authorized user rejection but keep out unauthorized users. However, in practice you'll be using the same templates for both access control and signing electronic records, and this latter process needs to work well with few errors with the biometric signing otherwise user rejection of the system may occur. This obviously has to be balanced with the acceptance rate being set sufficiently high to reject unauthorized users.

Specifically, the security logs of the system will need to be monitored for failure rates and the system acceptance rate needs to be fine-tuned if necessary.

Using Biometrics?

There are several questions about biometrics that I'd like to pose to you.

- Should we use biometrics in the chromatography laboratory?
- Are we ready to use biometrics?

Interesting questions you'll agree.

First, if your chromatography data system (CDS) is defined as a closed system, there is no need to use biometrics, as a unique combination of user identity and password is sufficient.

Second, there are also a number of practical considerations to assess before biometrics is to be used routinely in the laboratory. Do you use gloves when working in the laboratory to protect yourself from biological or chemical material? If so, you'll not want to use fingerprint scanners. In addition, the impact of chemicals and solvents on the

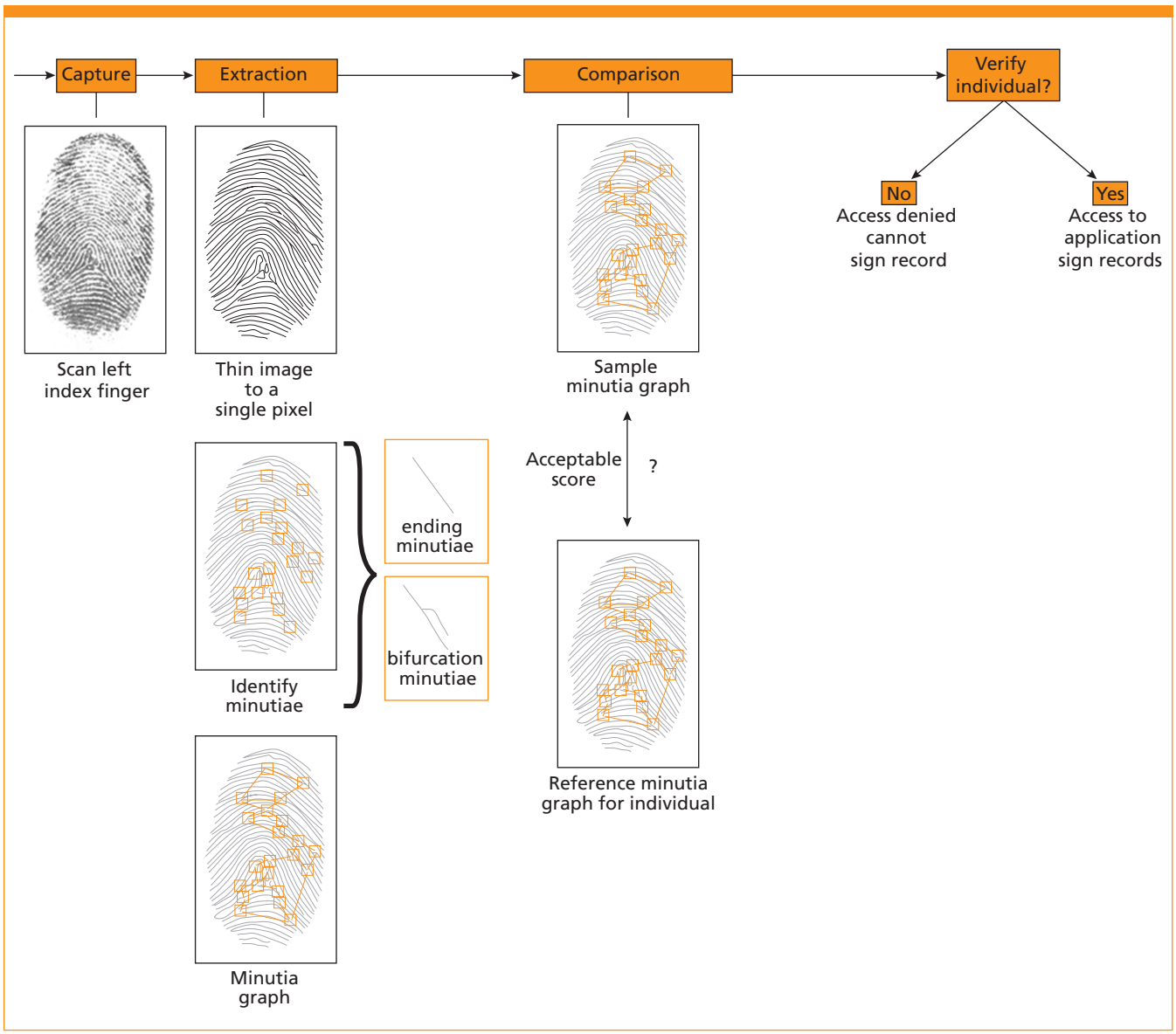

Figure 2: *Fingerprint scanning.*

skin of your fingers may be detrimental to fingerprint biometrics. Consider using alternative biometric devices such as face recognition or iris scanning: will they cope with protective glasses or hair protection used in some manufacturing or biological areas? Failing that, what about using voice recognition? This could be useful providing that background noise in some areas doesn't affect the false acceptance or false rejection rates.

I don't want you to get the idea that I'm against using biometrics but you have to consider the practical application of the technology before you end up with an expensive failure on your hands. Just don't be seduced by technology.

References

(1) R.D. McDowall, *LC•GC Europe*, **13**(5), 331–339 (2000).

(2) Enforcement Policy 21 CFR Part 11: Electronic records; electronic signatures (Compliance Policy Guide 7153.17) Federal Register 64 (1999) 41 442–41 443.

Bob McDowall is Visiting Research Fellow in the department of Chemistry at the University of Surrey, and Principal of McDowall Consulting, Bromley, Kent, UK. He is also a member of the Editorial Advisory Board of LC•GC Europe.