

**Abstract** There are many popular assumptions around biometrics and what a biometric identity check really means. Some of these assumptions properly belong in the world of mythology. This chapter clarifies exactly what a biometric identity verification check actually means and how it works technically, covering factors such as matching thresholds and degrees of likeness. Similarly, there exists a degree of misunderstanding around the finer points of individual biometric techniques and their principles of operation. The primary biometric techniques are therefore clarified and placed into perspective. Applications are also discussed with respect to biometric functionality and associated aspirations. This chapter consequently provides an overview of biometric technology, explaining how the technology has evolved, how it works and what it may and may not provide, exploding a few myths along the way. It explores how identity verification has developed as a separate function from early access control systems and looks at some of the currently popular biometric techniques, exploring their strengths and weaknesses accordingly. This chapter provides a solid foundation for those which follow, ensuring that the reader has an adequate working understanding of the technology upon which to develop further thinking.

---

## Biometrics Defined

The word *biometric* means literally a measurement of life. Many years ago, the author offered another definition as follows: *A physiological or behavioural trait which may be measured, stored and thus utilised in subsequent comparison with a live sample for automated identity verification purposes.* This definition aligns well with the way we think about biometrics today and seems to have been universally adopted. It follows that there are potentially many biometrics although, in practice, just a few have endured as popular techniques for automated identity verification purposes.

Before we go any further, it is appropriate to clarify what a biometric identity verification check actually means and to address a few myths in this context. There is a fundamental distinction to make here between a one-to-one check, wherein we are comparing one stored biometric with one live sample, and a one-to-many check, wherein we are comparing one live sample with many stored biometrics. In the former case, we are seeking

to corroborate a claimed identity by comparing the live sample with a stored biometric, claimed to represent the individual concerned. In the latter case, we are seeking to identify the individual by comparing the live sample with a population of biometrics, in order to find a match.

When we undertake a biometric identity verification check, we are essentially comparing two sets of computationally derived, digital information in order to ascertain how closely they match each other (we do this many times in a one-to-many check). Of course, they will never match each other absolutely, due to natural variances in the way the live sample is presented, environmental conditions and a host of other factors. Consequently, we place a condition upon this match, effectively agreeing that a match has occurred if a certain threshold of likeness has been reached. In simple words, you may think of this in terms of a percentage. Any matching transaction result which falls beneath this threshold will consequently be seen as a non-match, and the transaction will fail. Therefore, a match is always a relative match according to the predefined parameters, which, if satisfied, we consider to represent a match. In the majority of systems, this set of parameters, or match threshold, may be adjusted. Therefore, at a specific point of presence, a system may be tuned according to local conditions. Figure 2.1 illustrates this. We shall revisit this idea later in the book. Suffice it to say that there are no absolutes with respect to biometric identity verification; it is always a question of degrees of likeness when comparing a stored biometric with a live sample. Even when comparing sets of stored biometrics, the same principles apply.

When we refer to a stored template, we should understand that this template could take a variety of forms. It may quite literally be an image of the biometric trait as captured by an optical device, or it may be a digital representation of the trait derived according to

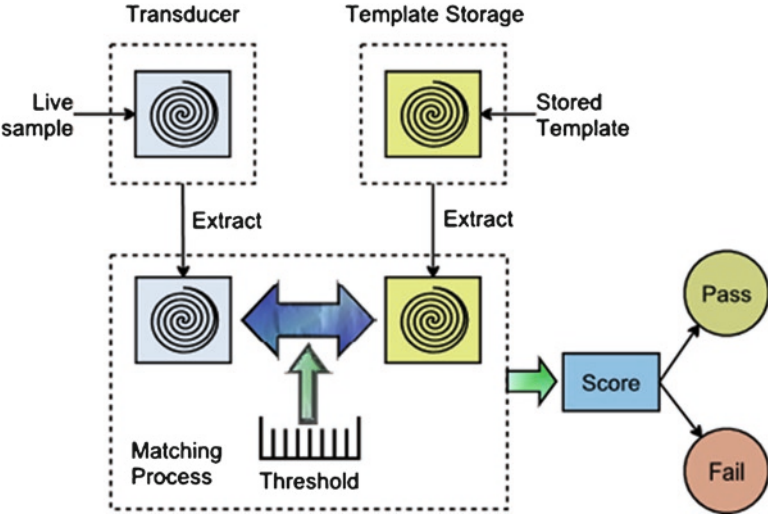


Fig. 2.1 A simplified view of the biometric matching process

vector or feature information. In either case, it is likely that a certain amount of processing will have taken place, both with respect to feature extraction and removal of unwanted noise. Such processing will be undertaken both at the time of template creation and at every subsequent matching transaction. It is possible therefore that the processing itself may, under different conditions, introduce a small amount of errors. Whether these errors are significant or not may depend both on the biometric technique employed and the precise configuration of the biometric transducer and matching algorithm. We shall consider other types of errors elsewhere in the book.

---

## Assumptions

Let us explore a few of the assumptions often made around biometrics and individual identity verification.

- A biometric match proves that I am who I say I am.  
Absolutely not the case; a biometric match proves nothing of the kind. It simply provides a level of confidence as to the likeness of two sets of information. Other information aligned with the stored biometric record may or may not be correct and may or may not have been edited or tampered with.
- A failed biometric transaction proves that I am an impostor.  
Incorrect. It simply shows that two sets of information have failed to match according to a predefined likeness threshold.
- A biometric check is infallible.  
Not at all; there are many factors which may conspire to give a false result, either a false positive or a false negative.
- Biometrics cannot be spoofed.  
Certainly some biometrics and associated devices are more resistant to others in this respect, but most have been successfully spoofed at one time or another.
- A biometric will protect my privacy.  
Absolutely not. Indeed, the opposite is often the case. In any event, such an assumption cannot be made out of context; it all depends upon the application and associated infrastructure.
- All biometrics are stable over time.  
Not necessarily the case. Some are certainly subject to change and others are more resilient. This factor, and the implications for live matching transactions, is often not well understood.

One could continue with a long list of assumptions and half-truths which are often claimed or promoted with respect to biometric identity verification. However, I believe that we have made the point that biometrics are not infallible and that we should beware of attaching too much importance to a biometric identity verification transaction in isolation. As part of an intelligent brace of measures and checks, defined in relation to the

perceived risk at hand, a biometric check may provide an increased level of confidence as to the identity of a given individual, providing the information aligned with the stored biometric is indeed correct in itself. If the associated information has been falsified, then the biometric check simply serves to augment the fraud. This is an important point which needs to be properly understood.

---

## Biometric Methodologies

Now that we have placed the value of a biometric check within a proper perspective, we might usefully consider some of the currently popular biometric methodologies and their associated development. Back in the 1980s when there was a lot of activity and research into what we would perceive today as contemporary biometrics, the focus was predominantly upon physical access control; in other words, gaining entry through a physical portal such as an internal door or external gate. In fact, many early systems were described simply as door entry systems. The electronic control was often centred around a keypad and personal identification number, although, often, even this was shared among all users. Keypads were slowly joined by card or token readers, which could be used either in conjunction with the keypad or in isolation. Cards became more sophisticated, the humble magnetic stripe card being joined by infrared cards, Wiegand cards and a variety of other tokens including short-range transponder cards for 'hands-free' operation. Developments in card technology were mirrored by increasingly sophisticated control mechanisms which could cater for hundreds of entry points and provide additional functions around alarm monitoring and building management.

The access control market consequently blossomed and many sophisticated systems became available. However, the concept was not without shortcomings. As systems became larger, card and token management became more of an issue. Furthermore, the instances of individuals passing tokens between them increased, throwing doubts upon the accuracy of transactional records. We may know that a particular token had been used at a given point of presence on a particular day, but we could not be absolutely sure that the individual using the token was the same individual to whom it had been assigned. If the system was additionally being used for time and attendance purposes, this was an unfortunate reality. In very high security access control scenarios, the limitations of tokens were particularly pertinent. If, however, we could incorporate a biometric check, either with or without a token, then we could surely have an increased confidence as to the true identity of the individual concerned. This was the driver behind most of the early, pioneering biometric systems. Indeed, many of them were physically implemented within an access control like architecture; one can recall early implementations of hand geometry, voice verification, fingerprint scanning and retinal scanning, which were effectively access control systems that happened to use a biometric rather than a token. Slowly, the biometric functionality divorced itself from the control functionality, although there are still examples where the two are usefully combined. Let us consider some of the popular biometric techniques.

## Hand Geometry

Hand geometry was one of the early pioneering biometric techniques that originally measured the position and length of the fingers when placed upon a platter surface. The original device was rather large and cumbersome, but this was soon refined into the ID3D hand geometry device (from Recognition Systems Inc., the primary advocate of hand geometry), which was much neater and, as the name suggests, introduced a three-dimensional factor via the use of mirrors. There were many strong points associated with this device, including relative ease of use and an unusually small template of around 9 bytes, facilitating its storage upon portable media as well as having low system resource usage if stored centrally or, as was possible, within the device itself. The ID3D was also well considered from a systems perspective, facilitating simple RS485 networks to be created with nothing more than the readers themselves and effectively providing distributed template storage. Current versions of the original hand geometry reader continue to provide good functionality, ease of use and a quite reasonable performance. They remain particularly well suited to certain types of applications and are often used in the context of physical access control, time and attendance monitoring, benefit provision and similar applications.

## Voice Verification

Voice verification was another early pioneer and there were a few different systems available for a while, some of them quite well considered from the systems perspective. Typically, voice verification systems analysed the individual dynamics inherent within the annunciation of a given pass-phrase, creating a template accordingly which could be used for subsequent matching with the live sample. While the theory is logical enough and, no doubt, some of the matching algorithms well developed, voice verification as a technique is disadvantaged in several ways. Firstly, if using commercially available transducers such as telephone handsets, the quality of mass-produced low-cost transducers is not only relatively poor in terms of frequency response and dynamic bandwidth, but notoriously variable from sample to sample. Secondly, we have the inconsistencies and noise within the communications channel (e.g. telephone lines, routers and exchanges) to consider. Thirdly, variable point-of-presence environments will have equally variable ambient noise levels and acoustic properties such as reflectivity, absorption, preponderance towards standing waves and so on. Lastly, the consistency with which users interact with the transducer device often leaves much to be desired, especially with non-habituated users. Such issues, when summed, can create enormous challenges for voice verification systems. Nevertheless, they may be well suited to certain, closed-loop applications where voice is the biometric of choice.

## Signature Verification

Signature verification as a technique was also among the pioneers and there were several competing systems at one stage. It seemed like an obvious application of biometrics as there were so many familiar processes that used a signature as a means of identity verification.

Furthermore, signature verification biometrics, in theory at least, provided a further depth of analysis as one could measure the dynamics inherent in writing the signature as well as the precise geometry of the signature. In isolated tests, signature verification could give a reasonable account of itself. However, in live situations, using commercially available graphics tablets and existing systems components, things were often not so easy. Furthermore, it is interesting, when considered in proportional terms, how relatively inconsistent some users are in signing their name, both dynamically and graphically. While a human observer might, even subconsciously, make allowances for such inconsistencies while still correctly recognising a signature, a signature verification matching algorithm has a harder time, especially when attempting to function within tight tolerance levels. Consequently, signature verification has yet to fulfil its promise as a viable mainstream biometric technique, although there may be applications where it could prove to be useful.

### **Keystroke Dynamics**

Keystroke dynamics is another early technique in which a great deal of time and effort was invested, including by some major information technology companies. The idea of recognising an individual by their particular keystroke dynamics was clearly an attractive one from an information technology and networks perspective. While it did seem possible to determine an individual dynamic signature under carefully controlled conditions, real users under real operational conditions were not perhaps as consistent in the way they used a keyboard as one would have liked in order to implement this technology. Furthermore, using standard keyboards, there wasn't really a wealth of individualistic information with which to work. After much research and some interesting demonstrations, the idea of keystroke dynamics as a viable behavioural biometric seemed to fade, especially when other techniques were seen to be making good progress.

### **Fingerprint Recognition**

Fingerprint recognition is probably the biometric technique which most people are aware of. It was always going to be an obvious choice of biometric for those in law enforcement, where matching fingerprints has been fundamental to the identification of criminals since the turn of the last century. This reality in itself initially introduced something of a stigma, due to the strong alignment with criminology in most minds. There is a dichotomy here between automated fingerprint identification systems (AFIS) as used by law enforcement agencies to search large databases, often off-line, in order to identify criminals, and discreet fingerprint biometric systems, which typically function in real time in order to verify an individual identity, within a range of scenarios. The two functions are increasingly interlinked in areas such as border control, and this raises some interesting questions.

The technology itself, however, has progressed quickly into workable systems which are considerably easier to use and more reliable than some of the original implementations. Fingerprint readers may use either an optical or capacitive sensor, each of which has their own advantages depending upon the application. Optical sensors may offer high resolution

and be easily able to capture a full grey-scale image of the fingerprint. Capacitive sensors tend to be smaller, easily integrated and less sensitive to the build-up of grime on the surface of the sensor. The fingerprint matching process may be based upon identifying minutiae according to a spatial vector, or may be based upon image matching by pixel contrast or grey level. Some systems may store both minutiae information and a full image of the fingerprint. In practice, fingerprint recognition has become well adopted as a biometric methodology across a broad variety of applications. Many of these applications are in the public sector, for applications such as border control, national identity documentation, benefit entitlement and so on. Many more are in the private sector for applications such as network access, mobile device security, voluntary transportation payment systems and other applications. Fingerprint sensors have become almost a commodity item and are often supplied on an original equipment manufacturer (OEM) basis for incorporation into laptop PCs and a variety of other devices, as well as being provided in a range of distinct forms as commercial off-the-shelf (COTS) products for integration into other bespoke systems. The performance of fingerprint recognition can be robust, depending upon the number of fingerprints utilised and the dependence upon human and environmental factors.

### **Retinal Scanning**

Retinal scanning was a pioneering biometric technique, developed initially for access control purposes within military environments. Its performance could be very good under certain conditions. However, its usability was typically rather troublesome, at least with respect to early implementations, although it improved a little in later iterations. This is primarily because usage originally involved peering into a binocular device and aligning one's vision upon a target – something that many people initially struggled with, especially those with impaired vision. In addition, many users did not very much like the idea of physical contact with the binocular interface. Consequently, while usage within a controlled military environment may have been acceptable (largely because such users had no choice in the matter) the technique found little favour within the broader community. The retinal scanning technique involved scanning the vein patterns on the retina with a low-powered beam shone into the eye: an intrusive function which was not typically considered an attractive proposition by potential users. Furthermore, early versions of retinal scanners were prohibitively expensive for anyone outside of the military. Later versions became much less expensive and were rather better considered in terms of connectivity, systems integration and the user interface. However, by then, other biometric techniques had found a wider acceptance and had effectively marginalized retinal scanning as an operationally viable technique.

### **Iris Recognition**

Iris recognition has become a popular biometric technique and is generally recognised as being perhaps the most accurate technique in terms of matching individual iris patterns. Consequently, it is a useful technique both for one-to-one matching for the purposes of

individual identity verification, and one-to-many matching for the purposes of identifying a particular iris from within a large database. In addition, the relative operational performance of iris recognition can be very good. In early implementations, failure to acquire an image of suitable quality under real operational conditions could be an issue, as could acquiring high-quality reference templates. However, the technique quickly evolved and such issues are rarely troublesome today. Iris recognition readers tend to be rather more expensive than those for certain other techniques, largely because of their relative complexity. Furthermore, installation and commissioning may be a little more demanding, especially with regard to environmental placement and the accommodation of a broad range of individuals of differing physical size. Such deployment issues may be overcome, however, and may be considered insignificant for applications where the accuracy and performance of iris recognition is required.

In simple terms, the technique typically involves locating the iris within a human face, separating it from the pupil and sclera, dividing the visible iris into segments and analysing each segment accordingly. From this analysis, a relatively sophisticated iris code may be derived and matched against a previously stored reference. The amount of detail represented within the iris code allows for a high degree of confidence when undertaking matches, even when searching very large databases. This is facilitated by the amount of available information that may be derived from a typical iris, and the relative uniqueness of the iris within the human population. Indeed, even the left and right irises of the same individual tend to be distinct and irises are considered to remain stable throughout life, being fixed shortly after birth. Iris recognition has grown in popularity in recent years and is a technique which will no doubt continue to be widely used.

## Face Recognition

Face recognition has been available as a biometric technique for a long time, although it is probably fair to say that early implementations left something to be desired in terms of accuracy and reliability of matching. However, the technique has many potential applications and continued development ensured that it quickly matured into a viable operational technique. Typically, the technique involves metrics of, and between, distinct features within the face, relying less on factors of a transitory nature such as hair style or the use of cosmetics. Nevertheless, the human face is subject to change over time and this reality will remain a challenge for face recognition systems, as will variance of expression, illness and other natural factors. In addition, environmental and human factors will almost always play a part in the efficacy of a face recognition system within a given deployment scenario. Consequently, face recognition may not quite match the accuracy provided by certain other techniques. However, it lends itself readily to applications where the face is already used within an identity verification context. Similarly, the ability to match against a stored image, perhaps from a different source, will appear attractive in some public sector applications. Face recognition has occasionally been used in conjunction with another biometric in order to increase confidence in the identity verification process. Face and fingerprint is a popular combination in this context. While not offering superlative levels of accuracy or operational performance, face recognition nevertheless remains a popular technique, and one which will no doubt benefit from further development.



## **Gait Recognition**

The potential attractiveness of gait recognition lies in the ability to recognise an individual at a distance. However, there are serious challenges to be overcome in this respect. The idea that an individual typically walks with a unique gait is an interesting one and, under laboratory conditions, the concept of gait recognition can be demonstrated. However, real life is full of dynamic variances which render the implementation of such a system particularly difficult. In addition to the complexities of matching, there are factors such as the opportunity to even capture the moving image of an individual in isolation and in sufficient detail to be able to undertake such a match. Creating a reliable template is also something which presents real challenges. Gait recognition represents an interesting example of biometric research driven by a perceived requirement: in this case, to identify an individual at a distance beyond which contact and near-field biometrics can function. While perhaps an attractive idea for military and very high security applications, it is doubtful that gait recognition will become a mainstream biometric technique.

## **Vein Scanning**

It has long been considered that the pattern of veins within the human anatomy may be unique to individuals. Consequently, there have been various implementations of vein scanning over the years, from hand scanning, to wrist scanning and, more recently, finger scanning. Most of these techniques have been shown to work and could certainly form the basis of a viable biometric identity verification system. The problem that they face is not one of technical capability or efficiency, but rather one of market realities. The preponderance of fingerprint, face and iris systems, readily available at a broad range of costs, makes it difficult for a distinct technique to gain market share without a clear and compelling advantage. Even early techniques such as hand geometry have an installed base which is unlikely to be impacted by a newer technique of comparable performance. Consequently, for any new biometric technique to become established in the marketplace, it must break new ground and offer clear advantages that cannot be realised by contemporary methods. The various implementations of vein scanning, while undoubtedly interesting, may struggle a little in this context. However, time may prove an interesting leveller in this context and distinct applications for vein scanning may appear.

## **Other Techniques**

There are various other biometric identity verification techniques which have surfaced from time to time, including ear lobe recognition and scent recognition. Almost any anatomical feature or behavioural trait might be deemed a candidate for an operable biometric. However, we have to place such ideas in context and align them with the perceived requirement. If this requirement is to have a method by which we might verify an individual identity with a reasonable degree of confidence, then the existing biometric methodologies provide us with the means to do this in a variety of ways, thus facilitating a broad range of applications. Perhaps, in time, other techniques will be developed which might supplant

some of the existing methodologies. For now, we might usefully turn our attention towards a better use of existing techniques within contemporary applications, and the provision of a better understanding of the future alignment with societal expectations. Such matters will be discussed within these pages.

---

## Which Biometric Is Best?

A question that is asked perhaps more than any other in this field is which biometric technique is the best? The answer of course is that there is no *best* biometric in absolute terms, it all depends upon the precise nature of the application and the reasons for its implementation. In order to get a feel for this, it is pertinent perhaps to consider a few obvious application areas.

### Physical Access Control

The original application for automated biometric identity verification, physical access control, remains a viable application for this technology. Several techniques have been used in this context, such as fingerprints, hand geometry, face recognition, retinal scanning and iris recognition. Important factors to consider include relative durability of biometric sensor devices, overall ease of use and desirability of a low false negative rate, whereby few individuals will find themselves blocked in error. Another factor has often been the integration with tokens such as conventional access control cards. In this respect, both hand geometry and fingerprints have been used quite successfully. Integration with existing systems, such as access control or building management systems for example, may be important in some cases. This will necessitate the use of a commonly used interface as well as a workable storage of biometric reference templates, either centrally, distributed among the devices themselves, or, ideally from both a performance and management point of view.

If a simple access control system is required within a new build scenario, then there are a variety of biometric-only systems, often based upon fingerprint technology, which may be easily deployed and commissioned and which will function quite well in an internal office environment, for example. Hand geometry can also work well in such scenarios. For high security access control applications, iris recognition would be a good choice, providing the sensing devices suit the environment. For example, under military or custodial scenarios, devices would ordinarily be required to be ruggedised and tamper-proof. External applications present their own challenges, particularly in harsh environments. Interestingly, voice verification has sometimes been used in such applications, via ruggedised and weatherproof handsets. The choice of a biometric for physical access control must take all such factors into account. Of course, available budget and the implications for ongoing maintenance will also factor strongly in many such situations.

## **Time and Attendance Monitoring**

Time and attendance monitoring is a relatively specialised application area with a long history of using tokens, from punch cards to access control cards. It is also, these days, strongly driven by software, integration with payroll systems and flexible reporting functionality. Consequently, it is often the case, when implementing biometrics, of integrating biometric sensors with an existing system. Fingerprint readers have been used quite successfully in this context and there are also various dedicated fingerprint systems available. Another biometric technique which has found much favour for this application is hand geometry. Indeed the flexibility and connectivity offered by the leading hand geometry device lends itself well to such applications, as does the relative usability of the technique. Iris recognition would no doubt also work well, although the cost and operational methodology may not appear so attractive in certain environments. Time and attendance is one application area where contact-based techniques tend to be well accepted.

## **Logical Access Control**

Logical access control, across computer networks and even within specific computer applications, is an area traditionally managed by a combination of user name and password. However, for higher security when a second factor is required, a biometric can work very well. Interestingly, this is an application area which has failed to grow in line with expectations, in spite of a plethora of low-cost fingerprint devices as well as various software-based techniques such as face recognition which can interact with existing transducers such as the webcams incorporated in many laptops. Perhaps part of the reason for this lack of adoption is the dichotomy between single device access and network access. For single devices, the user name and password methodology has become somewhat ingrained and is generally held to offer sufficient security. For network access, the necessity for integrating seamlessly with directory services may have deterred many from adopting a biometric. In addition, the question of support for a large user base in the event of persistent false negatives, for example, is no doubt one of concern for many organisations as this would be seen as a potential increase in support costs, especially if users need to be re-enrolled with their biometric. Nevertheless, it is possible that we shall see growth in the use of biometrics for logical access control. Factors such as business-to-business connectivity and the increasing reliance upon IT for many organisations in both the public and private sectors, coupled with increasing concerns around data security, may reawaken interest in this area. There was a time when it looked like capacitive fingerprint readers would soon grace the lines of almost every laptop computer, although relatively few models are thus equipped at present. More ubiquitous is the presence of an imaging device, both on laptops and monitors. Assuming an adequate resolution from such devices, perhaps a form of iris recognition might eventually find its way into this area at a low enough cost to make it viable. That would certainly be an interesting development. In the meantime, there are various fingerprint readers that may be easily integrated for those wishing to explore this area.

## On-line Transactions

An extension of logical access control across public networks such as the Internet provides many business opportunities. It also has implications for security as many organisations have found to their cost. Applications such as on-line shopping and, importantly, on-line banking are increasingly becoming the norm, as are on-line interactions with public agencies. Encryption can go some way to protecting sensitive data, but access into external networks and onto external servers is always a worry, particularly access at administrator level. If a miscreant obtains the necessary identity credentials, he or she can wreak havoc in many ways, from simply stealing data to bringing down servers or even entire network segments. Furthermore, when such credentials are simply in the form of user names and passwords, their discovery may be relatively easy for a skilled miscreant. In theory, a biometric might serve to increase security within such a scenario, including that around non-repudiation. However, there are many factors to consider, especially around where the biometric is stored and at which point identity verification takes place. In this respect, it may be pertinent to consider access control within the hosting application quite separately from that of the remote client. Usability also has a part to play, as many customer users might struggle to understand and work with biometric identity verification. However, administrator access within the hosting network might well be an area worthy of investigation, although there are many issues to address. Indeed, the choice of a biometric technique may appear almost trivial compared to the challenges of designing an architecture which represents a genuine increase in security via the use of a biometric, while remaining workable and supportable. Once such challenges have been overcome, the biometric techniques of choice will no doubt be similar to those for internal network access control.

## Portable Device Access

The rise in the use of portable devices has been pronounced in recent years. Furthermore, the functionality has become somewhat blurred, with devices which started out as mobile phones becoming, in effect, miniature personal computers, cameras, web browsers, data storage devices and general on-line communications devices. Mobile computers themselves have adopted a wide range of wireless connectivity functionality and may themselves operate as mobile communications devices. Even the form factors have moved closer together with the advent of the netbook PC and increasingly compact notebook PCs, all featuring cameras and often preloaded with a range of social networking software. One result of this mobile technology revolution is that such devices may hold a good deal of personal information. Indeed, modern netbook and notebook PCs have more data storage capacity than would be found on some servers not so many years ago. As such devices may easily be mislaid or even stolen, security becomes increasingly important, especially for devices issued to corporate users. It will be interesting to see how biometric technology will be used in this context. Already, one can easily incorporate face recognition into devices with an integral camera. Fingerprint sensors are small enough to be included, even in the smallest PC form factors, and they are to be found occasionally on notebook and laptop PCs. Whether such options become popular and commonplace will no doubt depend

upon the suppliers and what they perceive as their primary market. However, there is certainly scope for intelligent implementations in this sphere, perhaps for corporate remote workers, for example.

### **National Identity Documentation**

National identity documentation, in the form of identity cards and passports, is an obvious area for the adoption of a biometric, especially with the adoption of chip-cards and chips in passports. This opportunity has not escaped the attention of government agencies and there are now many implementations around the world. Fingerprints and iris recognition are popular methodologies, particularly fingerprints as these can very easily be referenced against other databases, including criminal databases if required. There is an interesting paradox here as the concept of a national identity document historically has been to affirm the right of an individual to cross a border according to their country of residence and whatever international agreements are in place. Consequently, the primary use of a biometric should be to confirm that the individual presenting the document is the same individual to whom it was originally issued. This concept has become somewhat blurred as the national identity document and the biometric it contains is being used increasingly for law enforcement purposes. Perhaps this is symptomatic of the times we live in. In any event, embedding a biometric into such a document is easy enough. The controls around registration and the processes by which such a document will subsequently be used will require careful consideration, as will the physical and technical reality at the point of checking. As a consequence of the almost universal use of fingerprints for law enforcement purposes, it is likely that fingerprints will predominate on national identity documents, although iris recognition and face recognition have been allowed for within the relevant document standards.

### **Border Control**

Border control is an interesting area. On the one hand, some authorities may be satisfied with a simple biometric check of the user against the biometric reference embedded in the national identity document. Others, such as the USA for example, may require the collection of biometric data quite separately and will check these data against criminal databases, as well as storing it for future usage. Furthermore, they may require a much more extensive collection of biometric data, such as all ten fingerprints. Biometric data may also be used for VISA applications, enabling the checking against criminal databases before a VISA is granted, and also ensuring that the VISA user is the same individual who provided a biometric at the time of application: a useful application of biometric identity verification within the auspices of border control. Given the close association with law enforcement, it is perhaps not surprising that fingerprints predominate as a biometric technique in this area, although there are exceptions, with iris recognition in particular proving popular in this area due to its inherent accuracy. For border control purposes, it is often not essential to align the biometric with a national identity document, and various interesting schemes are in operation with or without an associated token.

## Benefit Claims

Being an obvious application for biometric identity verification, it is surprising that the technique has not been used more often to control benefit fraud, especially in countries where this is a major issue and a major cost for government. It is a simple matter to issue claimants with a token containing a biometric and then check this biometric for each claim. With thorough background checks undertaken at the time of registration, such a system would no doubt provide impressive efficiencies and cost savings, as indeed has happened in areas where the concept has been introduced. Fingerprints would be an obvious biometric technique due to the relatively low cost of implementation and comparative ease of use. However, other techniques could be adopted if, for example, a non-contact methodology was preferred. As with any public sector implementation, it is the attendant technical architecture and operational process which will require careful consideration if such systems are to realise their potential benefits. The concept could be utilised across a wide range of state benefits and associated scenarios.

## Industrial Processes

The use of biometrics with respect to industrial processes, such as when sophisticated machinery needs to be operated by certified trained operators, or in relation to very high security installations, may be an area where biometrics can prove extremely useful. In such applications, a non-contact, accurate methodology such as iris recognition might work well. Alternatively, under certain environments, a robust technology such as hand geometry might also be suitable. It is an area with many possibilities for creative thinking around the use of biometric identity verification. Furthermore, when aligned with safety, it would represent a valuable use of biometric technology. It will be interesting to see how things progress in this context, and one might expect to see an increasing use of biometric identity verification in this area over time.

## Other Applications

There are countless potential applications for biometric technology: anywhere, in fact, where a strong confidence is required as to the true identity of an individual either performing a specific function or claiming a particular benefit. Clearly, there are areas where it would simply not make any sense at all to add the complexity of biometric identity verification to an existing process. It should be remembered that it is not simply the biometric matching process which needs to be designed, but the whole end-to-end process including registration, support, ongoing maintenance, data management and so on. There are also areas where the adoption of biometric identity verification might make considerable sense. That is for implementing agencies and individuals to decide. This section has perhaps served to illustrate that there is no single *best* biometric technique. It is a question of the application, the operational environment, the user profile and what we are trying to achieve. Furthermore, it is easy to become preoccupied by the characteristics and theoretical performance of different

biometric techniques when the focus should really be upon clarity of purpose, sound technical architectures and properly considered operational processes.

## Considerations Around DNA

Whenever biometrics are discussed, the thread often meanders its way, sooner or later, to DNA and the possibilities of using DNA as a mainstream identity verification method. There are many reasons why this is currently not really viable, not the least of which is the time and specialised facilities required for DNA analysis. However, it is appropriate that we consider DNA within these pages and provide a simplistic overview accordingly.

DNA stands for deoxyribonucleic acid and is the fundamental fabric of genes which, joined in a long string, make up the human genome. It is made up of nucleotide base pairs, each consisting of a purine and pyrimidine, and there are around 3.2 billion base pairs in the human genome. There are around 30,000 functional genes, that is, those that encode proteins, within mammalian genomes, including the human genome. Proteins are encoded by a transition process from DNA to mRNA (messenger ribonucleic acid), a specific sequence of which encodes a particular protein according to the genetic code.

As illustrated in Fig. 2.2, the encoded protein will depend upon the precise sequence transcribed from DNA into mRNA, a sequence which could be taken from anywhere within the genome. Furthermore, even this same sequence may be transcribed slightly differently as introns are discarded and molecules attached to the exon sequence, resulting in different protein coding. Considering the size of the genome and the degree of inherent randomisation, these processes may become highly complex. Indeed, while there remains much we do not, as yet, properly understand with regard to molecular genetics, it is clear that this DNA sequence is far from being fixed. We understand, for example, the process of exon shuffling, which can create new genes. Similarly, via a process of transposition, entire sections of

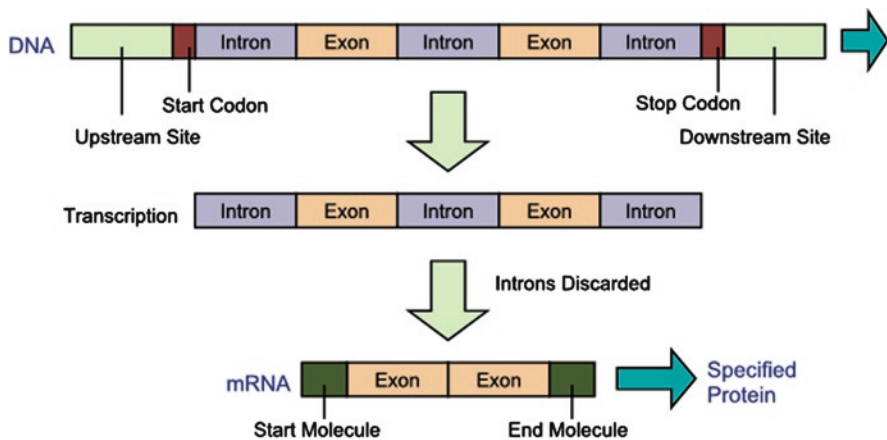


Fig. 2.2 A simple view of the DNA transcription process

DNA may be randomly copied and re-inserted at different points along the genome. Indeed, it is currently supposed that around 45% of the human genome consists of repeated sequences and that there exist around 4.3 million repetitive elements which we call microsatellites. This, of course, is all part of the process of mutation, which is a natural component of evolution. Genes mutate from one form, or allele, to another in order to create phenotypic effects. It is this very flexibility which allows for species to adapt. It is estimated that human babies have around 300 mutations which neither parent shares.

This very brief, high-level overview of DNA and its part in the evolutionary process reminds us that the genome is not some fixed, static entity, but a complex dynamic mechanism which can, and does, change. DNA can be damaged by chemical and physical events and altered by random mutations, all of which will result in sequence changes of one sort or another within the genome. DNA and genome analysis is thus a highly complicated affair and it is clear that we are still developing our understanding in this area. Consider, for example, the randomisation that triggers certain genetic sequences which ultimately prove to be harmful in humans (and other animals), often expressed as specific diseases which appear as if out of nowhere, often with no consistency as to age, gender, or ethnicity. This is simply the complex genetic mutational mechanism at work, and it starts with DNA.

Currently, there is a dichotomy of opinions emerging as to just how unique DNA may or may not be. Furthermore, the DNA analysis process is highly complex, exacting in its execution and subject to changing methodologies as our knowledge in this area develops. The common view of DNA as the ultimate personal identifier is consequently challenged as we increasingly understand the complexities involved. Those who dream of a commercially available, real-time DNA identity verification system might do better to employ their little grey cells, for the time being at least, to perfecting the comparatively simplistic mechanisms of biometrics. Mutation among said grey cells may of course overtake them in this quest.

---

## Review Questions

1. Discuss the automated biometric matching process and the purpose of a variable matching threshold.
2. Review and discuss the relative strengths and weaknesses of individual biometric techniques.
3. Distinguish between retinal scanning and iris recognition as biometric methodologies and discuss relative usability.
4. Review and discuss the potential for biometric identity verification for the purposes of network access control.
5. Discuss the practical relevance of DNA as a potential automated identity verification method.



Guide to Biometrics for Large-Scale Systems  
Technological, Operational, and User-Related Factors

Ashbourn, J.

2011, XIII, 201 p., Hardcover

ISBN: 978-0-85729-466-1