The Story So Far

2

In the previous chapter, we have discussed the origins of biometric identity verification and the primary application areas which have driven the development of the associated technology over the past 20 years or so. It will be useful for the reader at this stage to look at some of the applications and attendant issues in a little more detail.

One of the early implementations of biometric identity verification was retinal scanning. This involved scanning the retina with a beam of infrared light in order to expose the vein pattern on the back of the retina which was considered unique to the individual. In order to accomplish this, alignment between the transducer and the eye was critical and users were required to look into a binocular receptacle and focus upon a spot. This was hardly an intuitive way to verify identity in order to gain access to a facility or other benefit. Furthermore, spectacle wearers were at a disadvantage as they would typically need to remove their spectacles in order to interface with the retinal scanning device. Those with very poor close vision would then be at a disadvantage when using the device. However, retinal scanning was considered an accurate identity verifier and, consequently, systems were installed in high security application areas, mostly in the military domain. In such cases, users were positively required to use the system, regardless of any personal reservations they held about the technology. This perceived intrusiveness, coupled to the relatively high price of the original devices, ensured that retinal scanning did not find an immediate market outside of these niche applications. Eventually, the devices were refined and improved considerably and the cost dropped to a more accessible level, but by then, other techniques were becoming more widely accepted. Retinal scanning represents an interesting example of a biometric identity verification technology which, while exhibiting reasonable levels of accuracy, remained unintuitive in use and was consequently not embraced by users. Furthermore, the original devices were not well considered from a systems or network perspective, restricting their use in larger-scale applications. Later on, significant improvements were made in this respect, but it was a case of too little, too late. The same may be said of several current fringe techniques which may be interesting from a purely

J. Ashbourn, *Biometrics in the New World,* DOI 10.1007/978-3-319-04159-9_2,

technical or theoretical perspective, yet largely impractical for everyday use. The biometric industry has a talent for such technical serendipity.

Another early biometric technique was hand geometry. The earliest devices were large, cumbersome affairs with sliding pins to separate and locate the fingers. These worked tolerably well, but were clearly not very practical from an installation and user perspective, being much too large and cumbersome. However, the design of the leading contender was quickly refined into a much smaller device with fixed pins which made use of a carefully placed mirror and an LED light source in order to realise a three-dimensional representation of the fingers, within a sheltered alcove. This was a much more elegant device which was also quite intuitive in use, with the user simply entering a PIN in order to retrieve their template from the device's memory store, and then placing their hand on the platter surface. Furthermore, the device was compact, easily installed at entry points and contained its own networking capabilities via an RS485 connection. It additionally featured a dry contact input and a relay output, with rudimentary configuration via a two-line LCD display. In other words, this device had been designed from the outset with practical usage and connectivity in mind. Consequently, it began to define its own market, largely for physical access control into secure areas. However, the flexibility of design enabled additional functionality and the devices also found a ready market for time and attendance applications and other specialist areas. Card readers could be attached to the hand geometry device and, as the biometric reference template was compact—just nine bytes, it could easily be stored upon a magnetic stripe card and recalled from the token if desired. Alternatively, large numbers of reference templates could be stored within the device in nonvolatile memory or shared among a network of devices. In addition, the primary hand geometry reader exhibited the ability to learn with regular use, continually refining the template for habituated users, thus becoming more accurate over time. This was a good example of flexible design and a willingness to adapt which suited the early hand geometry readers to a variety of applications, including one of the first border control applications, implemented as a voluntary service for frequent flyers at several airports in the Americas. Interestingly, hand geometry readers are still used at airport locations for physical access control applications. They also remain in use for time and attendance applications, entitlement verification within schools and public service areas and elsewhere. A good example of a technique which has proved adaptable across a variety of applications and is thus enjoying a longevity which has eluded some of the other early biometric techniques.

In parallel with such developments, a wide variety of fingerprint readers were being developed and launched into a market area which seemed to have almost as many suppliers as users. Initially, most of these were optical readers, using imaging components to capture an image of the fingerprint which could be processed by an attendant algorithm in order to create a reference template. In some cases, this template was itself an image, in others a mathematical representation based upon the position of identifying minutia within a grid of coordinates. These early devices came in a variety of shapes and sizes and often featured a simple RS232 connection for integration within a broader system, or direct connection to

a computer. Others were their own contained system, aimed squarely at physical access control, and included template storage, networking and the necessary relay outputs with which to integrate into a door entry system. Some even emulated a Wiegand access control card, in order that they be easily integrated into existing distributed access control systems. However, some of these early designs lacked the robustness necessary for use in industrial or heavy usage environments, where the exposed physical surfaces would quickly become contaminated. Slowly, capacitive sensors started to appear, which enabled fingerprint readers to be made more compact or even integrated into other devices. This was a step forward and, when the Universal Serial Bus (USB) system was introduced to computers, compact capacitive readers with USB connectivity became available at much more affordable prices. However, to some extent, fingerprint biometrics, outside of AFIS systems, remained a technology looking for an application. There were no end of designs launched into a theoretical marketplace that had yet to mature, and too many suppliers claiming outrageous performance figures which were rarely realised in practice. The market would need to rationalise and become more flexible in order to sustain such a technology. This is exactly what happened, with a fewer number of device manufacturers serving a diverse market, mostly consisting of systems integrators, developing innovative applications based upon fingerprint biometric technology. These were often in the area of entitlement, and often in association with another token, such as a plastic card. For a while, many laptop computers, targeting the corporate marketplace, included an integral fingerprint sensor which could, if required, be used as an access control methodology. While this may have been attractive to some individual users, there was little integration with corporate wide directory systems and, consequently, little uptake among large organisations. Furthermore, claims that their usage would somehow reduce help desk calls due to forgotten passwords, did not hold much water as, in many cases, passwords were still used and, in fact, help desk calls due to users having difficulty using the biometric device would likely be significant in their own right. Slowly, fingerprint readers started to disappear from laptop computers. A similar situation existed with fingerprint sensors built in to computer keyboards. The concept worked well enough, but there was little enthusiasm from either users or corporations. Currently, we are seeing biometric identity verification being promoted in relation to mobile devices such as smartphones and tablets. It will be interesting to see how this concept is received by both private users and organisations where the devices might be used. The likelihood is that this development will serve to reawaken interest in biometrics in general and fingerprints in particular. Meanwhile, there remain a significant number of defined applications which rely upon fingerprint biometric technology. The concept is well understood and the available transducers are easily integrated into broader applications. In addition, matching algorithms have developed to a point where a good balance has been achieved between accuracy and usability. Certain techniques, such as those based upon subsurface imaging, additionally offer a potential operational robustness which earlier designs lacked, and some offer a liveness testing capability, in response to the threat of using dummy or severed fingers (although, just what the probability of

such usage really was is somewhat hard to quantify, but it has been known). The variety of available readers, coupled with easy integration has enabled many bespoke applications to be developed which use fingerprint biometric identity verification. These range from frequent traveller systems, event access and entitlement to library systems and welfare. In addition, fingerprints have been incorporated into many official documents such as drivers licenses and identity cards. Fingerprint biometrics represent an interesting example of continuing technology and product evolution within a complex and varied market.

When iris recognition was first introduced, the available readers were complicated and expensive. Stand-alone devices being much too large to be discreetly integrated into operational environments. There were also some early hand held devices, although these required special computer cards for image processing purposes and were similarly expensive. Initially, iris recognition was not an easy technique to master. However, it was quickly acknowledged that the technique worked well with generally superior levels of accuracy. It was inevitable therefore, that this performance advantage would eventually ensure a place for iris recognition technology. Furthermore, and unlike retinal scanning, this was a non-contact technology which did not impose too much of a burden upon users. One simply had to look towards a camera device. In time, these devices became considerably more compact and employed better technology for locating the iris at a distance and, if required, taking rapid multiple images in order to perform a matching transaction. The technique also lent itself to one to many database searches, and it was this feature especially which helped to develop the market for iris recognition among larger-scale applications. It became possible to search quickly through large datasets in order to find a matching biometric. This, in turn, provided ease of enrolment without necessarily tying the biometric to a token. New reference templates could simply be entered into the database. Furthermore, this approach made it easy to use biometrics anonymously, simply requiring a match or non-match, without knowing who the subject actually was. This functionality is well suited to access control and entitlement systems where the user base may be both varied and transient. New implementations of iris recognition have been appearing in recent times, and most seem to function well. Original patents are now expiring and we shall likely see a new raft of products and ideas featuring this technology.

While iris recognition has been an attractive choice for reasons of accuracy and functionality, face recognition has been popular for reasons of expediency. Many official documents such as passports, driver's licences, identity cards and criminal record documents incorporate an image of the users face. It would seem intuitive, therefore, to use face recognition to match such images. In addition, there has always been the desire to pick out faces in a crowd and match against a database of facial images. Unfortunately, such functionality has, at the time of writing, proved less than reliable, Even straightforward one to one matching of a live face with a stored reference image has challenges due to the fact that faces change over time, sometimes deliberately so. Even plotting coordinates such as eye centres, position of the nose, head width and so on is no guarantee of success. Furthermore, in real world deployments, incident light, shadows and reflections can serve to complicate

the situation and make accurate matching somewhat temperamental, a factor which may easily be exploited by those with an interest in defeating the system. That is not to say that the technology does not work. It can work very well with a contained user base under controlled conditions, but, historically, some of the claims made by technology suppliers have proven to be a little ambitious. From a positive perspective, matching algorithms have steadily improved with variations including three-dimensional facial recognition among others. In short, there are applications where face recognition can work quite well and others for which it would not be such a good choice. It is also a technique where user factors may have a significant impact, and these will be discussed later in this work. Face recognition remains a popular biometric technique however, due largely to its relative ease of implementation coupled to an intuitive operation. We are, after all, used to recognising each other by facial features, so why not replicate this in technology? It is also a technology which, in rudimentary form, may easily be integrated into almost any device which employs a camera element, as do smartphones, tablets and other mobile computing devices. This may appeal to a new generation of private users in a way that other techniques have hitherto failed. The future for biometric face recognition will no doubt be a bright one as the technique, in various forms, will find its way into a broad cross-section of applications of various facilities. It may not be the most accurate of biometric verification techniques, but it has a ready appeal which will ensure its future in many areas. However, many humans have remarkably similar faces which even serve to confuse human recognition. The greater the human population, the more pronounced this issue will become. Furthermore, individual faces change over time, sometimes to an alarming degree, and this rate of change is also variable among individuals. Other changes are transient, for example, those experienced as a result of severe illness or stress. Some might argue that the basic coordinates such as distance between eye centres, length of nose and overall shape of the skull, remain constant. But this simply is not true. Everything can change, including the shape of the skull. Coping with this variability is a challenge which we must acknowledge and take into consideration when implementing facial recognition biometrics.

We could go on to discuss many other techniques, some of which have endured and some of which have disappeared. These include voice verification, gait recognition, several variations of vein recognition, ear lobe recognition and even scent recognition. However, with finger, face and iris biometrics offering sufficient flexibility to meet the majority of operational requirements, the need for other techniques is perhaps questionable, although, no doubt, they will continue to appear periodically and usually with outrageous claims as to their overall performance and usability. One technique which may well see a resurgence of interest however, is voice verification. It has been somewhat hampered to date by the relatively poor quality of transducers and attendant processing, not to mention the disparity among voice networks and the interference which sometimes ensures. However, these architectural factors are improving all the time and there undoubtedly exist applications which lend themselves very well to the concept of voice verification. Technically, in a carefully controlled environment, it is a technique that can work well. Furthermore,

it is one which may usefully be used in association with other techniques, perhaps as a second factor for occasions when there is some question as to the performance of the primary factor.

This brings us on neatly to the controversy surrounding multimodal biometrics and whether such an approach really offers any practical benefit. There are proponents both for and against the idea. Those in favour believe that two (or more) biometrics must be better than one and therefore, stand a better chance of correctly verifying individual identity. Those against argue that performance can only be as good as the best performing biometric mode and that adding a secondary mode simply confuses the issue, especially when one factor succeeds and the other fails. From an off-line identity verification perspective, having more than one biometric trait available will be seen as beneficial, especially in borderline cases. However, this is not the same activity as a live multimodal biometric identity verification. For live verification purposes, it is the view of the author that a properly implemented single mode biometric identity verification system, will offer as good a performance as may reasonably be hoped for. Of course, much depends upon the biometric technique chosen. Two poorly configured and unsuited techniques will not magically offer better performance in a real world operational sense, due to their being combined. Furthermore, the vagaries of matching thresholds and template quality may well work against any theoretical benefit in this context. Those with an interest in mathematics and probabilities will be intrigued to find a similar dichotomy of opinion from that perspective. No doubt the controversy will continue. However, the concept of using multiple biometrics is already being practised within some high profile applications.

A Change of Direction

The above discussion serves to illustrate, in simple terms, how the popular techniques have found their market place. Things might have continued along a meandering evolutionary path, with suppliers coming and going as they did so often in the early days, were it not for the events of September 2001 which, effectively, changed our world forever. The sense of outrage over the terrorist attacks in New York and Washington ensured that public sector identity management adopted a new complexion. Consequently, measures to incorporate biometrics into passports and identity cards were given a new sense of urgency and border control agencies started to develop their own databases of biometrics collected from travellers and, in most cases, referenced against criminal databases. The efficacy of this approach is sometimes questioned in terms of fighting terrorism, but the effect for the biometrics industry was akin to a rejuvenation. Suddenly, large funded contracts were available to support the development of associated systems and suppliers were not slow to respond. Unfortunately, the landscape was complicated a little by the reality of large corporations securing contracts for which their technical understanding was limited, leading to an initial mishmash of associations and alliances with so-called specialist biometric companies.

However, this was probably inevitable as few had any real experience of such large-scale systems at this juncture. Consequently, a natural evolution took place as systems and components were refined in the light of increased large-scale experience. In parallel, operational processes were also refined in order to embrace the new methodologies and the challenges that they presented. Throughout this period there have been interesting claims and counter claims, both regarding the technology and the political processes involved. Curiously, there remain concepts and operational factors which are not universally well understood and therefore, constrain the potential of such systems. There is also the question of behind the scenes operations and to what extent the biometric technology serves to inform them. This is an area which shall be discussed later on in relation to big data and other information technology initiatives.

The large-scale applications around border control and national identity may have stolen the media headlines, yet smaller-scale, bespoke applications continued to be developed, often by smaller, more specialist organisations. This ensured that a diversity of biometric products continued to exist as alliances were formed and products matched to perceived application areas. This situation endures today, with many bespoke applications being designed and implemented using a variety of biometric techniques. Occasionally, these are punctuated by genuinely large-scale applications, often in the field of national identity, which tend to utilise the popular techniques such as fingerprint and iris recognition. In addition, a raft of new applications in the mobile technology space is opening up. This situation enables the industry to develop and diversify into these primary application areas. Supplier organisations will tend to be divided between those who offer proven, reliable technology which has evolved over time, and those who produce innovative ideas, embracing emerging technology and infrastructural trends. These will be augmented by the large, multinational business consultancies who are increasingly offering biometric identity verification within their portfolio. Among this mix of potential suppliers, much effort will be expended on differentiation and seeking to offer unique capabilities. Sometimes, these capabilities will be more aligned with integration than any fundamental improvement in the efficacy of biometric matching techniques. Furthermore, the tendency throughout the recent history of biometric identity verification deployment has been to concentrate rather too much on the technology, and rather too little on the attendant operational processes. The latter include a clear definition of what is being sought and why (clarity of purpose) coupled to a logical process for configuration at node level and the handling of exceptions. These processes should be supported by an in depth understanding of human factors and a comprehensive logging and reporting subsystem. These fundamental requirements are often not given the priority and attention they deserve. This is immediately evident in some of the poorer-quality implementations to be found today. It also represents a risk when biometrics are incorporated into other, proven technologies, such as smart cards for example. In such cases, there will often be too much focus upon the token and not enough focus upon the underlying processes and the reality of biometric matching under operational conditions.

Evolution

We have seen a somewhat erratic evolution of biometric technology over the past 25 years, with peaks of activity interspersed with periods of too many suppliers chasing unquantified markets. The huge focus upon border control and national identity, in turn spurred by the focus upon fighting terrorism (although there clearly exist other political agendas), has created a very significant market for biometric technology. Another potentially large, but subtly different market is emerging with respect to mobile technology and connectivity, and how this may be used by private individuals, as well as, perhaps some of the services that they connect to. We shall consequently see a raft of new products and ideas in this area in coming months and years, especially from the large suppliers of mobile devices who will be competing with each other to offer what is perceived as innovative technology. Organisations who have applications in the cloud and are used to the concept of remote working, will wonder how these devices, and the technology which they embody may be used, as will suppliers of on-line services. All manner of federated identity ideas will surface, many claiming to successfully integrate biometric identity verification. The degree to which they can intelligently integrate biometrics into this landscape will vary significantly and there will exist a good deal of misunderstanding in this respect.

Across all of these areas, there exists the danger of making assumptions around the efficacy of a biometric matching transaction, without really understanding what is happening at a lower level. This lower level includes both technological and human factors. The author has undertaken a good deal of research in these areas over the years and has introduced several important concepts accordingly, supported by a significant body of published papers. And yet, the assumptions persist in many areas. In fact, the situation is likely to become more prevalent as biometric technology adopts a higher profile in the public perception. In parallel, there will be genuine advances at a lower technological level, but these will need to be properly aligned with operational process and the broader developing situation. One of the aspirations of this book is to encourage and support a better understanding of this reality. Large-scale, public sector applications have been mentioned and these continue to grow in their scope and operational scale. This, in turn, generates another set of issues which need to be properly understood and managed. Some of these are technological while some are of a more social nature. Others concern background operations such as intelligence sharing, which are partly informed by the widespread use of biometric identity verification technology. In such cases, incorrect assumptions may adopt an altogether more serious complexion and have unexpected implications. This is precisely why the practical application of biometric technology must be understood in context. At present, this level of understanding is not as pervasive as perhaps it should be.

Chapter Summary

In this chapter, we have explained briefly how biometric technology has developed in recent years, in alignment with external events and perceptions. It is a trend which is likely to continue as we witness an increasing use of biometrics across sometimes disparate applications. The idea of biometric identity verification becoming a commodity technology has been suggested for many years and, indeed, some product offerings have worked towards this goal. However, we continue to see new developments, sometimes aligned with new external trends, sometimes revisiting older ideas, suggesting that innovation continues in this area. The perception may be moving towards biometrics as a commodity technology to be simply 'dropped in' where required. The reality is rather more complex and implementing agencies need to be cognisant of this fact, if they are to deploy meaningful, sustainable systems. Furthermore, there are broader issues which surface as the technology is utilised on an ever increasing scale within the public sector. Consequently, a deeper understanding of biometric identity verification technology and its practical application needs to be developed. The brief overview of the popular techniques and how they have evolved serves to illustrate this reality. We have therefore discussed this background and how it has led us to the present position. We have also mentioned concepts such as multimodal biometric identity verification and the arguments for and against this idea, and we have covered the step change in the use of biometrics following the events of September 2001 and offered a few thoughts on future evolution. We have drawn attention to the fact that a detailed understanding of biometric technology and the way humans interact with it is not as widespread as it should be, given our aspirations for the technology. This is a particularly relevant observation at the current time as new applications are appearing rapidly. Furthermore, awareness of biometric technology among nonspecialists will undoubtedly be increased as a result of the integration of biometric functionality into mobile devices. This, in turn, will lead to increasing proposals for the use of biometrics in the workplace. Against such a backdrop, this chapter reminds us of the reality of biometric devices and the biometric matching process.

http://www.springer.com/978-3-319-04158-2

Biometrics in the New World
The Cloud, Mobile Technology and Pervasive Identity
Ashbourn, J.
2014, XXI, 236 p. 12 illus., 11 illus. in color., Hardcover
ISBN: 978-3-319-04158-2