Biometrics, Is it a Viable Proposition for Identity Authentication and Access Control?

Hyun-Jung Kim

Computer Security Research Centre, London School of Economics, Houghton Street, London, WC2A 2AE, UK.

In modern society, where a welfare recipient signs up for benefits under six identities, a child is released to a stranger from a day care centre, a hacker accesses sensitive databases, and a counterfeiter makes copies of bank cards, a trustworthy means of identifying employees or customers is urgently in demand. Biometrics is emerging as the most foolproof method of automated personal identification in today's highly computer dependent world. Biometric systems are automated methods of verifying or recognizing the identity of a living person on the basis of some physiological characteristics or some behavioural aspects. No one biometric system is likely to dominate the marketplace since all have limitations that compromise possible system solutions. The trade-offs in developing such systems involve hardware cost, reliability, discomfort in using a device, the amount of data needed, and other factors. This article looks at different types of biometrics systems and discusses in detail the various security implications associated with their application.

Introduction

There is now an increasing dependence on computer systems in almost all aspects of business and commerce and many organizations rely on the effectiveness of their systems in order to succeed. Increasing emphasis on computer security means that only authorized users should be allowed to access the information stored in the systems. One area where technology is enhancing and simplifying the process of identifying people is biometrics. Biometric systems are automated methods of verifying or recognizing a living person on the basis of some physiological characteristics, such as fingerprint or iris patterns, or some aspects of behaviour, such as hand writing or keystroke patterns [1,8,12]. Although computerized biometric devices have been around since the early 1970s, they were not commercially viable, mainly due to the expensive chip technology. Today with more affordable microchips, biometric devices are moving into commercial organizations and could challenge the growing use of smartcards as alternatives to passwords [19].

Background to Biometrics

Identity Authentication Methods

The conventional method of preventing unauthorized users from access to computers, entry to buildings and the use of banking terminals, etc., is by the use of identification and verification. There is a difference between information needed for unique identification. and the verification of a claimed identity [8,13]. First, identification (or recognition) requires the system to scan through many stored sets of characteristics and choose the one that sufficiently matches the characteristics of the user presented. In fact this resembles the way the human brain carries out most day-to-day ident-

0167-4048/95/$9.50 © 1995, Elsevier Science Ltd

ification tasks. However. unlike the brain where the recognition process is relatively quick and efficient, for computers, this is very complex, time consuming and costly. The second method concerns verification of a claimed identity. This requires the person being identified to state his/her identity, so that his/her characteristics presented are compared with the named identity (in the database), allowing the system a binary choice of either accepting or rejecting the person's claim. This article deals with the verification of a claimed identity, rather than the recognition of the identity of the user, since the identity verification task is simpler and the results are usually more reliable.

Generic Identity Verification Schemes

There are essentially three types of identity verification methods [8,12]:

1) Verification of something known, such as password, PIN number;
2) Verification of something possessed, such as keys, ID cards; and
3) Verification of some personal characteristics, such as fingerprint or voice patterns.

The security level of a system can be enhanced by combining these classifications. Often computer systems use the first two of these verification schemes (e.g. possession of a magnetic stripe card together with knowledge of its corresponding PIN number for most ATMs). The third category deals with the concept of biometrics, which uses parts of body or unique individual behaviour as a means of identity verification. Strictly speaking, the term biometrics refers to the statistical analysis of biological phenomena and measurements, but it has become widely used in the security profession to describe technologies used for professional identification [5,6].

There are four basic steps involved in the application of such a biometric access system: i) capture of the users' attribute; ii) template generation of the user's attribute (i.e. enrolment); iii) comparison of the input with the stored template for the authorized user on request of access; and iv) decision on access acceptance or rejection [1]. Unlike other access control approaches such as password or ID card systems the biometric measurements are likely to vary on each user login. Variations can arise from environmental factors (e.g. temperature, humidity), from human factors (e.g. stress, perspiration), or from wear and tear on the measuring devices. It is important that the true biometric devices should be able to handle such variations to some extent.

Identity Authentication Based on Biometrics

Classification of Biometric Verification Methods

Biometric systems look at both physiological and behavioural characteristics of a living person. A physiological characteristic is a relatively stable physical feature such as a fingerprint, hand structure, retina vascular pattern, iris pattern or some facial feature — all of which are basically unchangeable and vary little in time. In contrast. a behavioural characteristic reflects a person's psychological states (i.e. affected by influences such as stress, fatigue, colds, etc.). However, it does have some physiological elements that can be used to characterise a certain feature. For instance, the most common behavioural identification method is a person's written signature, since society has relied on the hand-written signature to verify the identity of an individual for decades. Other behaviours used include a person's keystroke rhythms and speech patterns. Because most behavioural characteristics change over time, many system's need to modify their original reference template each time they are used. Thus. after many successful accesses, the template could be different (sometimes significantly) from the initial template, producing more proficient performance in discriminating the invalid user. Schemes that employ this method work best only when used on a regular basis.

On the whole, since the degree of intrapersonal variation is greater in a behavioural characteristic than in a physical characteristic, it is harder for developers of such behaviour-based system to adjust individual's variability. However, systems that measure physical attributes tend to be larger and more expensive, and the use in some applications may be considered threatening to users. Behaviour-based biometric devices are generally smaller in size, cheaper to implement and more friendly to use. Either technique provides a much more reliable means of authenticating a person than simple password- or card-based security mechanisms. Because of these differences, no one biometric system will serve all needs, and to be effective, it is necessary to apply different techniques in different situations. For example, a voice verification system may be used in executive offices while fingerprint based systems are installed in the computer rooms.

Factors Behind Biometric Approach

Technology components

Biometric approach presents the high technology solution to access control problems, comprising three basic components. One is an automated mechanism that scans and captures a digital or analogue image of a living personal characteristic. Another handles compression, processing, storage, and comparison of the image with the stored data. The third interfaces with the application systems. These three elements may be configured differently to suit various situations. A common issue is where the reference templates are stored: at a host computer, or on a card, presented by the person being verified. Unauthorized disclosure of biometric templates is a very serious matter for users, hence it is essential that some adequate security measures are applied to prevent such events.

Template generation

Whether it is based on a person's behaviour or physical features, all biometric systems require the user's co-operation at least in two stages: first, during enrolment to generate a reference template of his/her characteristics, and secondly, during logon where the user's pattern is scanned and compared with the stored template for that user. Enrolment is achieved by the user entering a series of sample references. The template is usually calculated as the average of these sample references, and is stored for later comparison when access is requested. During the verification process, a user enters his/her characteristics, that are then compared with the stored template. A high difference between the original template and the current test input would indicate that there is a good chance that the current user is an impostor, thus access is denied. A low difference represents that the user is genuine, and access would be authorized.

Error tolerance (or threshold) setting

The identification power of biometrics' performance is based on the measurement of two types of error, namely: Type 1 errors - False Alarm Rate (FAR); and Type 2 errors - Impostor Pass Rate (IPR) [5,8]. The balance between these two factors determines the success of the biometric device. If the threshold is set so as to make it harder for impostors (i.e. the tolerance is too low), some legitimate users may find it difficult to gain access. resulting a high FAR. Conversely, if it is easy for authorized users to gain access (i.e. the tolerance is too high), impostors may also slip through the system with relative ease, increasing the IPR. In other words, reduction in Type 1 error rates can be achieved only at the cost of increased Type 2 error rates.

Therefore, setting the right threshold regarding the environment of the system, is a critical issue. Normally, an IPR value greater than 10% would be unacceptable, since an impostor pass implies a breach of security. However, a FAR value of about 5% is certainly acceptable, since a user would, on average. fail to access a password system 1 out of 20 attempts. Nonetheless. in any case, all biometric systems must have the ability to reset the threshold to increase or decrease the level of security as necessary.

Physiological Biometric Systems

Face

Using the features of the whole face for automatic identification is a difficult task because facial appearance tends to change all the time. Variances would be caused by different facial expressions, changing hair styles, head positions, camera angles, lighting conditions, etc., and create images that are different from the image captured earlier. Despite all these difficulties involved in facial recognition, there have been many approaches to use facial recognition, ranging from neural network pattern matching systems to infrared scans of 'hot spots' (or most constant features) on the face.

Growing interests in the approach include law enforcement agencies who are keen to have a machine that could recognize a known terrorist, drug dealer or bank robber in a crowd. physical security officers who could add extra value to their existing closed-circuit television systems, and computer security personnel who could incorporate a small video camera into PCs that would constantly check that the person sitting at the machine is the authorized user.

Face Example - NeuroMetric (NeuroMetric Vision Systems Inc., Pompano Beach, FL, USA)

This face recognition system is based on the pattern matching abilities of neural networks. It can recognize faces with as few constraints as possible, accommodating a range of camera scales and lighting environments along with changes in expressions and facial hair using different head positions. The NeuroMetric System was first introduced in 1992 and it operates on the IBM compatible 386-486 PC, with a math co-processor for number crunching, a Digital Signal Processor (DSP) card and a frame grabber card that is used to convert raster scan images from a camera into pixel representations. The images are captured in real-time. The software running on the DSP card finds the face in the scanned video image, scales and rotates it to the desired position. compensates for lighting differences and performs calculations to reduce the information to a set of vectors. These are input to the neural network, which compares it with the stored image. The system is trained repeatedly, until it learns all the faces and consistently identifies every image [8].

Fingerprint

Stability and uniqueness of the fingerprint are widely recognized, and identification techniques based on fingerprint have been in use by the police since the late nineteenth century. Today, as well as military facilities (e.g. The Pentagon) and government laboratories, banks (e.g. Barclaycard is experimenting with fingerprint and retina scanning [20]), jails and commercial organizations are among early adopters of fingerprint verifiers.

In verifying a print, many systems analyze the position of details called the minutiae. such as endpoints and junctions of print ridges. Modern systems also look at other major features for unique verification, such as the arch, loop and whorl that appears in the finger. For example. some devices count the number of ridges between the minutiae to form the reference templates, whereas other systems treat it as an image-processing problem, and apply customized Very Large Scale Integrated (VLSI) chips, neural networks, fuzzy logic and other technologies to solve the problem. Also, a number of systems are available offering integration with smart-cards for template storage that the user would carry. Such systems rely on the security of the card to prevent tampering.

In a machine system, the reader must minimize the rotation of the image. It must cope with slight variances with the stored image. Also, there exists problems when the user has minor injuries on the finger. In order for it to succeed, fingerprint recognition systems must overcome the stigma of their use in law enforcement applications. However, some systems actually build on this mystique to enhance the seriousness of identification

Fingerprint Recognition Example - Identix System (Identix Inc.)

The Identix Fingerprint Recognition System uses a compact terminal that uses light, lens and charged-couple-device (CCD) image sensors to scan a high resolution image of the fingerprint. It has a 68000 microprocessor with some custom designed chips for its calculations. The user is given a PIN number when enroling. Then, the user places a finger on the glass plate for scanning by the CCD image sensor. The image is scaled, rotated and translated to mathematical vectors that represents the fingerprint. To identify, the user enters the secret PIN number and places a finger on the glass plate for scanning. This image is compared with the fingerprint image of the template. The user is given three attempts for identification [8].

Hand

Hand geometry has been used in live applications since the early 1970's. There are several advantages in using the three-dimensional shape of a person's hand with an identification device. Firstly, it is reasonably fast. It takes less than 2 seconds to scan through a hand and produce the analysis results. Secondly, it requires little data storage space (e.g. ID3D Handkey system uses as little as 9 bytes, which can fit easily on magnetic-stripe credit cards). Also, only little effort or attention is required from the user during verification, and the authorized users are rarely rejected. The dimensions of the hand, such as finger length, width and area are the major features used for analyses. The one (technical) problem with systems employing hand geometry is caused by the rotation of the hand when it is placed on the plate. This could be solved using appropriate positioning of finger pins. Also, the system must take account of different hand sizes for different users, and its performance level should not be detracted by dirt and minor cuts in a person's hand.

Hand Example - ID3D Handkey System (Recognition Systems Inc.)

In this system. the user enters an identification code, and positions the hand on a plate between a set of guidance pins. Using a built-in video camera and compression algorithms, it looks at both top and side views of the hand. and the software compares the digitized image with the enrolled features to see if there is a match. The analysis is based on the measurement (of features including the dimensions of the finger length, width and area) and comparison of geometries between current and existing templates. To enrol, the system takes three hand readings. The average of the resulting vectors of characteristics is calculated and stored as the template. The user is also given the personal identification code. To verify, the user enters the identification code, and places his/her hand on the plate. The vectors of the characteristics of current hand are compared with the stored templates, and a score is produced based on the scalar difference between the two sets of vectors. A low score represents a good match. The ID3D recognition system updates new template's vector each time on each successful login, under the assumption that the original template is produced in less than perfect conditions.

The ID3D Handkey is widely used in the US. For example. at Kennedy and Newark International Airports it assists automated passport inspection and entry control of registered frequent international travellers. Lotus Development Corp. uses it to keep unauthorized visitors out of its day care centre [8].

Eye

The retinal blood vessel is highly characteristic of an individual. Retina scans, in which a weak infrared light is aimed through the pupil to the back of the eye, are one of the best biometric systems on the market, with low false alarm rates and virtually zero impostor pass rates [1,8,23]. The retinal pattern is reflected back to a chargecoupled device (CCD) camera, which scans the pattern. The image can be converted to less than 40 bytes of information. The major drawback for retinal scan technology Is by the users' resistance, since people in general, do not want to place their eyes close to the device that captures the image. The intrusive nature of the machine can be very discomforting.

Another device, which examines the iris, has the big advantage that it does not require the user to be near the device. In fact, it can operate even when the user is a few feet away. The machine focuses on the iris pattern, which is on the eye's surface. It was found that the iris has a highly detailed and unique texture that remains stable over decades of life. The observable features include contraction furrows, striations, pits, collagenous fibres, filaments, serpentine vasculatine, rings and freckles. Another advantage is that this part of the eye cannot be modified without causing damage to vision. It is also protected from damage by the cornea, and it responds to light, thus making duplicate artificial eyes useless.

Eye Example - IRISCAN (IriScan Inc. Mount Laurel, NJ, USA)

The IriScan system identifies the characteristics found in the iris of the eye. It uses a standard camcorder as the image source, a video frame grabber and a Sun SparcStation for calculations and analysis. The main problem with this system is to reliably find the iris of the digital image. This requires many mathematical operations. The zones of the analysis are determined, and the textural information (which contains the physical characteristics) is extracted. The information derived produces an Iriscode, which is stored as the file code, or template for future reference. The system uses Hamming distances between the Iriscode template and the Iriscode of the current image to determine the acceptance of a claimed identity. The Hamming distance can be considered as a measure of error (i.e. fraction of disagreeing bits) resulting from bit by bit comparison of the two Iriscode. If the fraction is small, the user is accepted as valid [8].

Behavioural Biometric Systems

Voice

One of the least invasive of the biometric recognition systems, and the most natural form to use is the speech recognition system. All the systems that analyze the voice are rooted in broadly based speech-processing technology. Most of the current systems require the user to speak a set of sentences to the speaker. The waveform of the sentences is measured using Fourier analysis to find the frequency spectrum that characterises the voice sample. Since people form their speech patterns through a combination of physiological and behavioural factors, imitation is impossible. However, there are problems with the conditions of the environment as computers find it hard lo filter out background noise. Other problems include the variability of voices due to the physical condition of the user and duplication using a tape recorder.

Voice Example - AT&T Smart Card Speech System

The AT&T Smart Card Speech system stores an individual's voice pattern on a smartcard. It uses a standard 386 PC with a custom built digital signal processing (DSP) card that digitizes the speech at 8MHz. To store a voice pattern (or voice print), the user needs to repeat a word (or a short sentence) several times. The spectral representations of each of the repetitions are analyzed, quantified, and the normalized to form about 20 variable parameters that include speed, pitch, energy, and density of the waveform. These values are stored onto the card. When using the system, the user would insert his/her smartcard into the slot, and talk to the computer through the microphone. The speech pattern is then analyzed to yield the parameters, which are used to compare with the parameters of the voice print stored in the smartcard. Access is denied if there is a large difference between the parameters [22].

Signature

The bio-rhythms needed to write a signature can be used in an automated identification system. The use of signatures is very wide and popular. All cheques are verified using signatures, the traditional method is by visual inspection of the written signature. There are two types of signature identification methods. One method examines the signatures already written, and compares it, as an image, with the signature template. The major drawback of this method is that it does not detect photocopied signatures. The other method is by the study of signature dynamics. This scheme looks at the dynamic process of making a signature — writing rhythm, contacts on the surface, total time, turning points, loops, slopes, velocity and acceleration. The devices used for signature dynamics are wired pens and sensitive tablets. The key in the recognition of a signature is to distinguish between the habitual parts from those that vary with almost every signing.

Typing Rhythms

Like a hand-written signature, typing rhythms exhibit the same neurophysical factors which can be used for unique identification of an individual. Typing rhythms schemes analyze the way a user types at a terminal by monitoring the keyboard inputs 1000 times a second. The normal method is to use keystroke latencies — the time lapse between keystrokes. Certain digraphs (or keystrokes of adjacent letters) often show unique timing patterns that can be used to characterise an individual. The general identification and verification procedure will require the participant to generate a keyboard reference profile (or template). On a later date, verification required the generation of a test profile, which is compared with the template. If there is a large difference between the two profiles, then the user is prevented from access.

Implications of Biometrics

User Acceptance

The previous section presented a wide range of biometric techniques that are currently either in use or being considered for future use. Clearly, one of the problems associated with introducing such techniques for identity verification is user acceptance. To be broadly acceptable, biometric techniques must be legally and physically robust, safe to use not invade the user's privacy, and not be perceived as socially unpalatable [5,6]. Therefore, certain methods, such as injected radio tags or tattooed bar codes used to identify pets and livestock, are obviously unacceptable. Many biometric security devices can be intimidating to users the first few times. For example, fingerprint scanners may be associated with the criminal bookings. Similarly, due to the inherent self-protection of the eyes, most people are likely to feel uncomfortable with the idea of having a laser directed at their eye retina every time they want to make a financial transaction[1]. In contrast, hand recognition where the palm is placed on the plate, appears not to

[1]. But in some cases, the psychological effect of the eye recognition can be beneficial, as it appears to be rather serious recognition method. which itself may discourage potential intruders.

bother people so much (probably because hand-shaking is common behaviour [8]). Also, dynamic signature verification would be acceptable to people of all ages and social groups who are literate, since signature is already widely used as a means of personal identification. In places where literacy rates are relatively low, other verification schemes related to voice, face or hand, may be socially more appropriate.

As with any other new system, user resistance to change is another concern for the biometric system designers. If the new biometric device is to replace the current system (in order to enhance the level of security), and to fit well in the existing organizational culture and environment, then provision for adequate user awareness and training programmes is crucial. The feasibility study should include user's concerns and requirements to understand what is acceptable to the user.

Performance

For potential users of biometrics in the areas of banking, government, health care and various kinds of businesses to appreciate the full benefits of the technology, it is essential that reliable devices are provided at affordable prices. As biometrics are based on probability rather than definite yes/no answers, two types of error may occur: rejection of an authorized user, or the incorrect acceptance of an unauthorized individual. False acceptance can mean fraud while false rejection can mean frustration. In Los Angeles county, the fingerprint recognition system has been operating for the welfare department's general relief scheme, involving 100 000 families [14]. It was claimed that use of the biometric system would save the county a considerable amount of money, but the system has shown only 95% effectiveness even though prints were taken from two fingers. This level of failure is probably too high for the UK, where there is a great dislike to identification cards of any sort. Cards linked to fingerprinting are particularly difficult, as they relate to images of criminal activity and a police state. Thus, it should be possible to adjust the threshold settings for acceptance and rejection according to the requirements of the overall application system, so that biometric systems produce the optimum performance.

Cost

Nonetheless, to be useful in the real world, the system should rarely reject authorized users and deter most impostors at a reasonable cost. Until now, despite the established performance of biometric devices in various access control applications, the high cost of biometric products has made them a rather expensive alternative to other automated security solutions. Careful adoption decisions by management must be based on the level of security required, cost/benefit assessment, risk analysis, evaluation of other system alternatives, organizational culture, legal aspects and various cost factors (such as operating cost, maintenance cost, and provision for user awareness and training). Indeed, it is vital to ensure that the benefit of using a biometric technique justifies the additional cost of introducing such a system.

Speed

In addition to maintaining the required performance level within the budget, it is important that the effective system should not allow any delay that is apparent to the user [5]. Biometric systems involve the user entering the measurement of some physical characteristic, followed by a comparison with the stored template. Since it is likely that more than one measurement is necessary, the overall verification process may be more time-consuming than the entry of a password or the insertion of an ID card into a reader. Indeed, the primary weakness of most available biometric systems has been a slow verification time. Although the enhanced computing power and improved data handling techniques will overcome this problem to a large extent, several seconds of verification time is still common in many security applications, which is undesirable for the user.

Security Loopholes

The fact that most physiological characteristics are almost impossible to alter, introduces another drawback to the use of biometric systems. For example, assume that a biometric system is being used for controlling access to a remote computer and that the user templates are stored on that computer. When a user who wishes to logon, enters his/her user identity at the terminal, the biometric measurements are transmitted to the host for comparison. This procedure would introduce at least two important potential weaknesses in the system: one relates to the database with the templates and the other to the transmission of the biometric reading. If an impostor were able to obtain either of these items of information, he/she could then impersonate that user. If this was to happen then it would be difficult to invalidate fraudulent claims and to protect the genuine user, as the user cannot easily change a 'biometric password'. This is a definite disadvantage compared with a conventional password based system where the user can easily change the password if it is felt to have been compromised. In fact, this can go further. For example, if the fingerprinting method is used and a user wants to access several computer systems, the danger of fraudulent access can be accelerated if any one of those systems is careless regarding either the transmitting or the storing of the templates. An impostor might get hold of information from one weak system that he/she can use to falsify the identity on all the other systems. Again since there is no (easy) way to change a user's fingerprint, it is a far more serious problem than the simple disclosure of a user's password or the misplacement of an ID card.

Danger of Misuse (Extended Use of Biometric Data)

In recent years, biometric technology has become remarkably advanced and its performance is far more accurate than any other forms of identification. Indeed, growing interests in biometrics technology is evident in many countries. Spain is planning a national fingerprint system for identifying unemployment benefit claimants. Russia has announced plans for national electronic fingerprint system for use by banks. Jamaicans will shortly need to scan their thumbs into a database before qualifying to take part in elections. and will need a smartcard to vote at the polling station. Blue Cross and Blue Shield in the US have plans to introduce nationwide fingerprinting for hospital patients [15].

The JFK project, called INSPASS (Immigration and Nationalization Service Passenger Accelerated Service System), has been operating since August 1993 as a voluntary system for frequent travellers. Many governments including the UK are monitoring the project. If the project is successful, the technology may eventually make conventional passports and ID cards redundant. However, as a trade-off for moving through immigration more quickly, passengers would have to accept a system that has the potential to create a vast amount of international transfer of their personal data. Ultimately, passengers might have to bear the consequences of event such as a universal immigration control system being linked to a wide range of other information sources, such as police and tax systems.

Indeed, the critical problem in this case arises when such a system is manipulated by governments and airline companies anxious to collect more information about the passengers. For example, a database of hand prints might be extended to illicit use by the governments for the population monitoring purposes. However, this seems to be rather harmless compared to more sophisticated secondary applications where the individual identity is cross-matched against other personal information including his/her biometric data, so that the combined information base becomes sufficient enough to draw a comprehensive personal profile. From the passengers' viewpoint, the consequences can be even more devastating in the countries like the US, where there exist no effective legislative controls to protect the public who become increasingly vulnerable to such an unintentional exposure of personal information.

To summarise, increased awareness of the possible consequences among the general public, together with government initiatives of tighter control and close monitoring of such rather unethical and reckless actions exercised by the third parties, are urgent to address the individual rights to privacy in the future. It is important to recognize that the individuals have ownership rights to their personal data, hence that they should be informed about data collection, and have right to decline use of a data by third parties [3,9,10].

Legal Aspects

A high-integrity identification scheme based on biometrics may universally be applied throughout the organization to control access to its valuable information assets. Integration of the biometrics with video, neural network pattern analysis, geographical information systems and other advanced technologies, have stressed privacy concerns in two ways: surveillance and personal data protection [9].

Basically, surveillance (or dataveillance) provides the raw data of who-is-where. There are significant benefits to be gained as a result of surveillance activities. For example, by recording and analysing an audit trail of each individual's patterns of actions, it may be possible for security personnel to spot any irregularities in an earlier instant, and thus to provide appropriate security measures to protect the organizational assets. Significant financial benefits may come from the timely detection and adequate prevention of various forms of abuse and fraud. Also, as mentioned earlier both government (e.g. tax and social welfare) and private sectors (e.g. airline companies) would benefit from cross-referencing the various types of information about the person, provided that an adequate matching scheme (involving biometrics) was used to minimize the likelihood of wrong identification. However, this raises sensitive issues of personal data protection. For example, continuous sampling of keystrokes patterns at employee workstations to monitor employee work habits and personal inclinations is problematic, particularly when the employee is unaware that such data is being collected. Dataveillance is, by its very nature, intrusive and threatening, hence an organization must justify its use, rather than merely assuming its appropriateness [10].

Many countries recognize both the political and emotional values of privacy protection and have adopted various strategies for achieving meaningful protection.

In the last 20 years, many countries have increasingly developed a set of guiding principles concerning collection, use and dissemination of personal information [9.10.21]. International conventions state that data should not be used for purposes (other than the original purpose of collection, except with the authority of law or the consent of the individual [10]. However, in jurisdictions where information privacy safeguards do exist, they are fragmentary, restricted in scope, and difficult to enforce. Fol example, the US Privacy Act has shown to be a weak protector of personal privacy. This was due to an exception, that permitted 'routine use' of data. It has been so widely applied as to undermine the effectiveness of the Act [9,20]. Similarly, the UK Data Protection Act of 1984 embraces some exceptions that fall outside the scope of the act. including any records held for the purposes of guarding national security, preventing and detecting crime, prosecuting offenders or collecting taxes [2,21]. Therefore, effective individual knowledge and consent mechanisms are necessary, both as a means of improving data quality (i.e. maintaining the integrity of data in case of mismatch), and to avoid unnecessary distrust between individuals and organizations.

Conclusion

Biometrics attempts to authenticate the user by measuring something unique to each user, such as fingerprint, voiceprint or signature. This requires special hardware that effectively limits the applicability of biometric techniques to comparatively few environments. Also. there are many social problems, one of which is the users' natural resistance to the intrusive nature of biometric devices. Moreover, people are very sensitive to the idea of having to provide personal characteristics. Another issue is that, while biometric techniques appear to be a very sound method for user verification, like all other approaches, the security actually achieved is highly dependent on the way in which that technique is used within any particular application.

Therefore. the success of biometrics can only be achieved if it is properly assessed and applied. Biometric designers must convince the public that biometric systems are safe, reliable and worthwhile. Synergy with state-of-the-art technology can help achieve this goal. The use of smartcards to store Biometric data avoids the need for host databases, instead relying on the security of the card to prevent tampering. It is also possible to incorporate a random challenge from the host in the protocol between the smartcard and the user, thus avoiding reply attacks. Moreover, biometric systems have the advantage that they demand less from the users since there is no need for the users to remember long password or go through complicated challenge and response dialogues. Effective user awareness and training programmes together with some adequate safeguards should follow in order to maintain the secure storing and legitimate use of such data.

To conclude, the problems mentioned above prevented biometrics from fulfilling their early promise. However, by overcoming these hurdles through proper assessment and planning, and by awareness programmes, biometrics will emerge as a powerful component in a wide variety of security applications.

Bibliography

1. CAELLI, W, et al., *Information Security Handbook*. 1994, England: Macmillan Press Ltd.
2. FORESTER, T AND MORRISON, P, *Computer Ethics: Cautionary tales and ethical*

dilemmas in computing, 2nd ed. 1994, London: The MIT Press.

3. DITTRICH, K, et al., *Computer Security and Information Integrity.* 1991, Amsterdam: Elsevier Science Publishers.
4. ANGELL, I. O AND SMITHSON, S, *Information Systems Management: Opportunities and Risks.* 1991, London: Macmillan Education Ltd.
5. SHERMAN, R. L, Bometrics Futures, *Computers and Security,* Vol.11, No.2, 1992, Elsevier Science Publishers Ltd.
6. SHERMAN, R. L, The Right Look Can Open Doors, *Security Management,* Vol.36, No 10, Elsevier Science Publishers Ltd. Oct 1992.
7. CHESWICK, W. R AND BELLOVIN, S. M, *Firewalls and Internet Security: Repelling the Wily Hacker.* 1994, Addison-Wesley Professional Computing Series.
8. MILLER, B, Vital Signs of Identity, *EEE Spectrum,* Feb 1994,
9. TUERKHEIMER, F. M, The underpinning of privacy protection, *Communications of the ACM,* Vol.36. No.8, Aug 1993.

10 CLARK, R. A, Information Technology and Dataveillance, *Communications of the ACM,* Vol.31, No.5, May 1988.

11. RUSSELL, D AND GANGEMI SR, G. T, *Computer Security Basics,* O'Reilly and Associates Inc.
12. JOYCE, R AND GOPAL, G, Identity Authentication Based on Keystroke Latencies, *Communications of the ACM,* Vol.33, No.2, Feb 1990.
13. PEACOCKE, R. D AND GRAF, D. H, An Introduction to Speech and Speaker Recognition, *IEEE Computer,* Aug 1990.
14. DALBY, S AND CANE, A, All fingers and thumbs - The search for a machine that reads prints, *The Financial Times (Technology),* 5 May 1994.
15. DAVIES. S, Forget the passport, let's see your hand: Biometric identification is putting an end to the long immigration queue, *The Independent (Computing),* 3 Oct 1994.
16. BURKE, N, Who will keep tabs on you?, *The Times (Information Technology),* 22 Jul 1994.

I7. *The European Market for Information Technology Security Products and Services,* Frost and Sullivan Inc, Summer 1992.

18. BARR, E, *The Control of Information Flow in the Workplace,* ADMIS Project, London School of Economics, Summer 1992.
19. MILES, R, Enemy Within, *Computing,* 3 Sept 1992, BCS.
20. ELLIS, S, Helping Captain Beanie beat fraud: Personal Finance, *The Sunday Times,* 27 Feb 1994.
21. WASIK, M, *Crime and the Computer,* 1991, New York: Oxford University Press.
22. BROWN, R, The Smartcard: A research report on systems, equipment, costs, advantages and markets, 1994, *Post-News.*
23. BOOKER, E, Retinal scanners Eye-dentify Inmates, *Computerworld,* Vol. 26, No. 12, 23 Mar 1992.
24. KRAYEM, R, Smartcards: A New Tool for Identification and Access Protection, *Security,* Vol.11, No.2, Apr 1988, Butterworth Ltd.
25. ROTENBERG, M, Inside Risks: Protecting Privacy, *Communications of the ACM,* Vol.35, No.4, Apr 1992.
26. DALY, J, Fingerprinting a computer security code, *Computerworld,* Vol.26, No.30, 27 Jul 1992.