DEFENCE
SCIENCE & TECHNOLOGY

Mar 2003

DSTO

Biometrics Technology Review 2002

T. Blackburn, M. Butavicius, I. Graves, D. Hemming, V. Ivancevic, R. Johnson, A. Kaine, B. McLindin, K. Meaney, B. Smith and J. Sunde

DSTO-GD-0359

DEFENCE
SCIENCE & TECHNOLOGY

Biometrics Technology Review 2002

T Blackburn, M Butavicius, I Graves, D Hemming, V Ivancevic, R Johnson, A Kaine, B McLindin, K Meaney, B Smith and J Sunde

Land Operations Division
Systems Sciences Laboratory

DSTO-GD-0359

ABSTRACT

The September 11 2001 terrorist attacks in the USA have motivated renewed global efforts to secure national borders and accordingly Australian authorities have demonstrated an interest in mechanisms that support these endeavours. This report examines the current state of biometric technologies, characterises the main categories and focuses on face recognition, which is the least intrusive but most effective means of applying filters at access points to the country. It also reviews some of the ramifications of large scale surveillance measures when applied to populations.

Published by

DSTO Systems Sciences Laboratory
PO Box 1500
Edinburgh South Australia 5111 Australia

Telephone: (08) 8259 5555
Fax: (08) 8259 6567

AR 012-602
March 2003

APPROVED FOR PUBLIC RELEASE

Biometrics Technology Review 2002

Executive Summary

This report examines the state of current biometric research, covering the literature up to October 2002. Due to rapid and continuing development of the biometrics area, it was difficult to decide when to stop. We hope to cover new developments in our next survey. This report reviews the active categories and the science employed in many of the production technologies, and depicts some of the application domains. It describes the basic technologies inherent in the four major taxonomies used in identification methodologies. These comprise authentication and validation approaches, each based on one-to-one and one-of-many models.

There is a description of the face recognition processes that are common to all of the different approaches. This includes the enrolment processes and the operations applied to captured data. The various sensors used in the data capture process are characterised and some signal processing techniques applied to the data are analysed. This analysis includes some of the algorithms and learning approaches, like neural networks, that have been employed. This is followed by a discussion of the matching processes that detail the true and false and the positive and negative matches and the relative value of the results of these analyses.

Descriptions of the most common biometric categories include a discussion of the strengths and weaknesses of each group.

Fingerprint technologies employ a number of different sensor types that produce two-dimensional maps of fingerprints. During the processing stage, the ridge patterns on the fingertip are often reduced to a digital representation for efficient storage. These technologies are practical and easy to implement but performance measures vary widely.

Face recognition technologies have many variables that can affect the performance of the sensors. This is due to the difficulties involved in capturing suitable camera images for processing requirements. Maps of the face are analysed, processed, stored and used in the matching processes. Performance levels for these technologies are not very high, with low processing speeds and varying levels of accuracy. However, these products represent the least intrusive technologies for application in areas such as airports and other observational areas.

Hand dimensions and palm and vein pattern analysis techniques are fast but limited in accuracy. Research efforts in these domains have a reasonably low profile.

Iris and retina scanning is claimed to be highly accurate but capturing suitable imaging samples is difficult and quite intrusive.

Voice analysis techniques have existed for a number of years but have found little favour outside of certain niche markets. The technology is inexpensive but still considered to be immature.

Identification through signature matching has been used for many years but is only valid in very limited and well-defined circumstances. There is also a trend towards the use of signatures for individual identification.

Keystroke, as a biometric, has advantages for the computer industry because no further hardware is required, however its adoption has been low due to its poor accuracy. DNA on the other hand has a very high accuracy but is limited in application due to it not being real-time. This is a major limitation for the majority of the verification and identification applications.

Using the shape of the ear as a biometric has recently obtained more research backing. As it is in its infancy, much of the detail concerning accuracy is unknown. For the purposes of user acceptance, cost, etc in this document, it has been deemed to be similar to that of face recognition.

The final major class of biometric technologies identified for review is work patterns. This is a young area and includes examples such as typing speeds, choice of words in a document and other individual characterisation approaches. Probably the first known example of its use was in World War II, when a British code-breaking team at Bletchley Park broke German 'enigma' transmissions; German operators would use the same words to set up the system rather than using truly random selections, enormously reducing the number of permutations. This is not an area that has attracted much research and has been considered as a potential backup to other measures.

Biometric applications include access controls to physical locations, equipment and computer systems with varying levels of security. Traffic management systems, machinery operating systems, including motor vehicles, and identification procedures in medical, military and government domains can also leverage biometric technologies.

System testing is a critical issue. It can be used to verify manufacturers' claims, to engender a level of trust in a system and to enable customisation in an application domain. Testing methodologies must be verifiable and robust.

Human rights and legal issues are examined briefly and the only research method in this area to date has been the use of surveys. More work is required in this area.

Reliability, security and veracity will become issues as biometric systems become more widely deployed. Standardisation on a local or global scale will be required to ensure effective deployment.

The report concludes that some biometric technologies are available for immediate use in certain domains and others may be become available soon. Widespread deployment will equate to reductions in acquisition costs and increased adoption of the technologies. In the following table we provide a summary of biometric technologies. The dimensions used to rate each biometric focal area describes categories of application usefulness. The scales used in each dimension evaluate each category in relation to the set of all categories used in this comparison.

Biometric	Finger	Face	Hand	Iris	Retina	Voice	Signature	Keystroke	Ear	DNA
Access control	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Surveillance	N	Y	N	N	N	Y	N	N	Y?	N
Accuracy	very high	high	high	very high	very high	med	med	low	?	very high
Reliability	high	med	med	high	high	low	low	low	low	high
Error rate	1 in 500+	no data	1 in 500	1 in 131,000	1 in 10 mil	1 in 50	1 in 50	no data	?	no data
Errors	dryness, dirt, age	light, age, glasses, hair	hand injury, age	poor light, contact	glasses, contact lenses	noise, cold weather	alter style	hand injury, tired	light, hair	none
False positives	highly unlikely	unlikely	very unlikely	very unlikely	highly unlikely	likely	likely	unlikely	?	highly unlikely
False negatives	highly unlikely	very likely	likely	very unlikely	highly unlikely	very likely	very likely	very likely	?	highly unlikely
Security	high	med	med	high	high	med	med	med	?	high
Stability	high	med	med	high	high	med	med	low	?	high
User acceptance	med	med	med	med	med	high	high	high	?	low
Intrusiveness	med	low	low	low	very high	low	low	low	low	high
Ease of use	high	med	high	med	med	high	high	high	med	low
Low cost	Y	Y	N	N	N	Y	Y	Y	Y	N
Standards	Y	?	?	?	?	?	?	?	?	Y
Strengths	existing databases in operation	surveillance, checkable by humans, can use existing equipment		high accuracy	accuracy	low cost, can be used for surveillance	low cost	low cost, no additional hardware required	profile imaging possible, surveillance use	accuracy
Weaknesses	public acceptance, environment -ally affected, specialised hardware	environment-ally affected, biometric changes	environment-ally affected, biometric changes, specialised hardware	public acceptance, glasses, specialised hardware	public acceptance, glasses, specialised hardware	accuracy	accuracy	accuracy	environ-mentally affected	not real-time, expensive, specialised operations, specialised hardware

Table: Biometrics comparisons summary

Contents

Figures

Glossary

CCTV Close Circuit TV

DNA DesoxiRibonucleic Acid

EER Equal Error Rate

ESD ElectroStatic Discharge

FAR False Acceptance Rate

FBI Federal Bureu of Investigations

FERET FacE REcognition Technology

FRR False Rejection Rate

FRVT2000 Facial Recognition Vendor Test 2000

FVC2002 Fingerprint Verification Competition 2002

ICA Independent Component Analysis

ID Identification

IR Infrared

LDA Linear Discriminant Analysis

PCA Principle Component Analysis

PIN Personal Identification Number

POS Point of Sale

RAND RAND Corporation

ROC Receiver Operating Characteristic

VNTR Variable Number Tandem Repeats

1 Introduction

Biometrics is the science of measuring the characteristics of human beings in order to identify them. There is nothing new in this concept [5], references in literature related to hand and fingerprints as a means of identification date back many centuries. Modern fingerprint analysis, for example, was promoted by Sir Francis Galton in the late 19th century. Today people continue to be identified by such measures as fingerprints, age, weight, height, sex and hair colour [30][129][132]. However, recent developments in sensors and signal processing have made it possible for new measures to be applied and for new levels of automation and classification performance to be obtained. Biometric technologies currently under development include work in the areas of fingerprints, faces, hand dimensions, palm prints, irises, retinas, vein patterns, voices, signatures, keystrokes, ears, DNA and work dynamics. We focus our interest on those technologies that provide immediate results.

Probably the most pervasive and potentially cost-effective biometric technology for the near term is based on fingerprint recognition. A variety of fingerprint sensors and processing systems have been developed to provide high quality, low cost identification of people. Where it is feasible to ask someone to provide a fingerprint sample, which can generally be done very quickly and with little inconvenience, this technology may provide highly reliable authentication of the identity of the owner. Fingerprint technology is likely to be increasingly widely used to control entry to select areas, to replace PINs for certain applications and to obviate the need for passwords to access secure computing systems.

Of the other technologies, face recognition is showing promise as an important, passive technique. The subject need not be aware that a biometric system is being used. Iris scans, retina scans and DNA may also produce highly reliable identification results for high security applications. Vein pattern, voice recognition, hand pattern, signature, keystroke and work dynamics may have niche applications, either as primary sensors or as confirmatory systems in conjunction with other means of identification.

The history of biometrics has followed the well worn route of new technologies, with an initial build up of excessive optimism followed by a trough of scepticism as the limitations become apparent. Most of the technologies are now approaching the final stage where realistic expectations lead to successful applications [108]. To date, most research appears to have been carried out on individual technologies, whereas it is possible that combinations of sensors can perform much more effectively than individual sensors. Research into this area is increasing and a number of technology houses have been established with the aim of implementing combined technology solutions [141][145].

Despite some successful applications, biometrics has some significant limitations. In particular, error rates remain relatively high for some methods, simply because all people are roughly the same. For example, all faces have the same basic eye/nose/mouth structure and numerous individuals in the world population will share a very similar geometry of these features. No face recognition system can be expected to resolve this fundamental overlap in the characteristics of different faces. Even in those areas where biometric measures are thought to be unique to an individual, e.g. fingerprint, retina or iris, the measuring process itself will often introduce uncertainties. The smearing of a fingerprint, for example, can significantly reduce the reliability of the measure. Thus, modern bio-

metric techniques cannot be relied upon as absolute indicators of the identity of a person and any application of biometrics must be designed with due allowance for the degree of imprecision in the chosen technology.

Another limitation on the widespread application of biometric systems may be triggered by the possible infringement of civil liberties. In some applications, such as access control to workplaces [108], subjects willingly submit to the scrutiny of biometric systems. However, there are applications such as unannounced crowd surveillance that may infringe civil liberties or generate other issues of a legal nature. Proponents and designers of biometric systems must take privacy concerns into account to ensure that such systems are not ruled out because they are seen to be in the "big brother is watching you" [117] category.

Despite the performance limitations and privacy concerns, it is likely that biometrics will become increasingly widely used. Many of the technologies should enhance physical and information security in an increasingly hazardous world and one of the drivers for the continued uptake of the systems will be the terrorist attack on the Twin Towers, 11 September 2001 [115][153].

There are only a few published examples of operational biometric systems. This is possibly because many users do not wish to reveal that they are using such technology. However it seems likely that biometrics will come into much wider use in the near future. This paper has been prepared to provide a survey of the current state of biometric technologies and to draw some conclusions on their potential future directions.

2 Biometrics Basics

There are many ways in which a biometric measure may be applied, but in general the technology will either replace or enhance existing security measures as in the following possible examples:

- a fingerprint scan may replace a password for a secure computer log-on [143]

- face scanning may replace a manned checkpoint allowing access to a military base [120]

- voice recognition software may authorise telephone commerce transactions [67]

- automatic handwriting recognition may authenticate cheque signatures [74]

- fingerprint signatures may authenticate the status of critical electronic documents [138]

- face recognition systems may assist customs operatives to screen incoming passengers [159].

Proponents of biometrics systems suggest that unless biometric methods deliver increased reliability and reduced cost they are unlikely to be adopted. The following discussion will focus on those applications and technologies that appear to have the potential to meet these criteria for adoption.

2.1 Biometric Applications and Processes

There are many different ways in which the various types of biometric systems could be classified. This review adopts a taxonomy based on application groupings that relate to the decision type and data size. This grouping has been chosen because, apart from obvious technology issues, the performance of biometric systems is determined largely by the scope of the classification regime, i.e. how many individuals must be compared. In general, the larger the number of comparisons made by a system, the better it must be at rejecting incorrect decisions. To illustrate the significance of the number of users, consider a hypothetical one-to-one fingerprint authentication of the identity of a mobile phone user. For a low cost system, the probability of generating a match to an incorrect fingerprint may perhaps be 1:1000 for individual prints. If the phone is stolen, the fraudulent user could try each of his/her fingers (each finger of the same person has independent fingerprint), so the match probability for that individual would be approximately 1:100 that at least one of his/her 10 fingers would produce a match. In combination with the low probability that an intending imposter will even be able to gain access to the phone, 1:100 may be sufficient protection. However, if the illegal user has a number of acquaintances who also try to use the phone, the chances that at least one of their many fingers will have a reasonable match to the authorised user's print may be quite high. If ten people try to use the phone, the probability that at least one of their hundred fingers will match with the stored data will be in the order of 1:10. This may not be acceptable and a higher performance identification system may be called for, or the system must be programmed to detect multiple illegal attempts to access the phone. This escalation of performance requirements with the number of required comparisons is consistent across all types of biometrics and it is valuable to define operating regimes based on this parameter. Requirements are situation and implementation dependent.

2.1.1 Verification

In the simplest verification application, the biometric system is called upon to answer the question "Is this person who he/she claims to be?" For example, credit cards are being developed in which the fingerprint information of the user is incorporated into the card so that transactions may be automatically verified [92]. The card will only allow transactions if the fingerprint data from the user matches that stored on the card. This type of application requires the comparison of only two data measures and a transaction may be allowed if the data indicate only a fair likelihood that the user is authentic [73]. The scope of the comparison problem is one-to-one, since it is limited to the comparison of two sets of data. A low confidence in the match outcome may be acceptable, since there is only a small chance that a single unauthorised user will have similar biometrics to the valid user.

Verification problems also include the class where multiple comparisons are required and the biometric system is required to answer the question "Which member of the known group is this person?" and a secondary question may be, "What is this person doing now?" It is assumed the subject is a member of a known group and the question, "Is this a member of the group", is not an issue. For example, early fingerprint techniques were used to manage payroll systems in large companies [9]. The biometric measure was used

to authenticate the identity of the particular employee to ensure that appropriate wages were paid. The scope of the comparison problem in this type of application is one-to-many, but the size of the "many" is limited to the size of the database of known users and intruders are excluded by other means. The absolute match confidence is not an issue and the biometric system must only choose the best match from its database.

Verification problems may also include the multiple comparison class where the biometric system is required answer the question "Is this person known to me and authorised to...". A secondary question, "What is this person doing now", could be used to track activities. Applications of this type include access control to secure areas or log-on to secure computer systems. For example, access to secure areas in an airport may be controlled by fingerprint sensors with the intention that members of the general public who accidentally or maliciously attempt to gain access are stopped but valid users are accepted. The scope of the comparison problem is one-to-many, but the size of the "many" is difficult to define and may be large, since it encompasses the database of the known group of authorised persons plus an undefined number of potential intruders. The absolute match confidence must be relatively high if the system is to ensure that all unauthorised users are excluded and all authorised users are accepted.

2.1.2 Identification (One-of-many Surveillance)

In this type of application, the task is to scan a very large population and answer the question, "Is there a subject of interest in this large group of people?". Airport surveillance to detect terrorists would fall into this category [144], where tens of thousands of people per day may need to be screened to look for a few people of interest who may present randomly and without warning. The scope of the comparison problem encompasses the relatively small group of persons of interest, plus the hundreds of thousands of people who may pass by the system in an operational period. This is an extremely difficult type of application since the chances that the biometrics of one of the known group will match the biometrics of at least one of the general public is relatively high and the biometric system must have an exceptional ability to distinguish between people if it is to be effective.

2.2 Pattern Recognition

All biometric processes require the comparison of measured data from a person with known data from a database [146] to determine if there is match. There are two basic approaches to the comparison problem; one is based on the step-by-step construction of the decision making process, an algorithm [11], and the other is based on the use of some form of learning mechanism in which the decision-making algorithm [52] still exists, but may be hidden from the user. Artificial neural networks [110] are typical learning mechanisms [29][96].

The following discussion focuses on algorithms in which the processing steps are clearly delineated in order to highlight some of the issues involved in the signal processing. There is much evidence that learning systems also tend to break up problems into discrete blocks internally, similar to the steps of mechanistic algorithms, so the significant issues for algorithmic approaches are also likely to be significant in learning based approaches as

well. Regardless of the classification method, all biometric systems have requirements for enrolment and operation as shown in Figure 1.

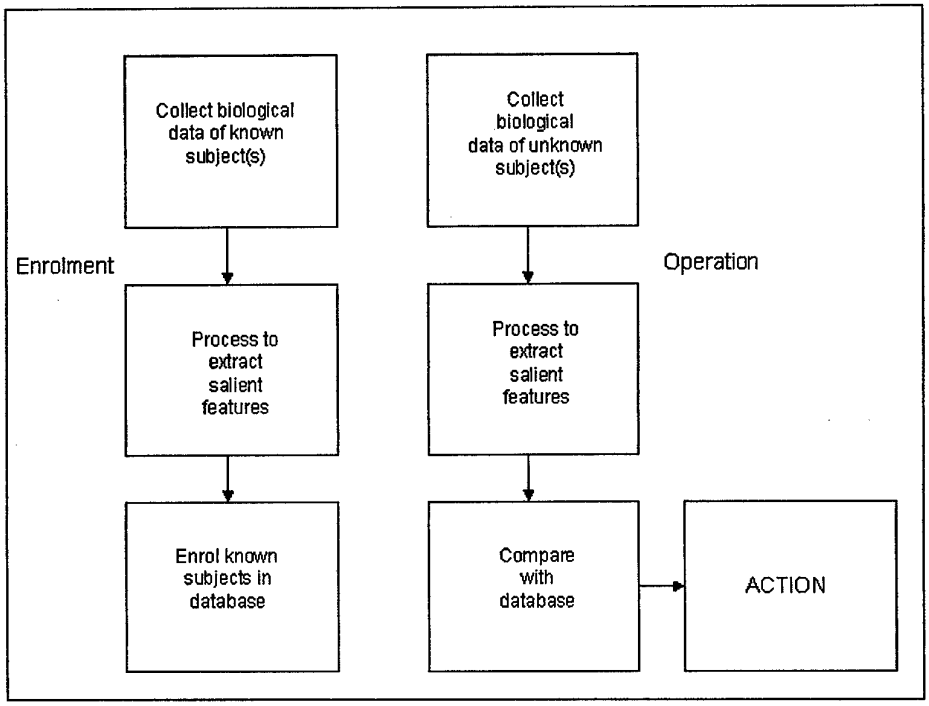

Figure 1: Biometric Processes

The two phases, enrolment and operation, use the same process to extract information from the sensor data [62][76][166][167]. In the enrolment phase, data on known subjects is extracted and is stored in the database [26][125]. In general, each individual will be sampled a number of times during enrolment to ensure that the stored data is truly representative of that individual. For example, a face recognition system may enrol a number of views of a person taken in slightly different poses to ensure that a wide range of possible views is incorporated [72][116].

When a database of known subjects is enrolled, which may be as few as one person in some authentication applications, the system may be used in the operational mode. In this mode, data from people who are not yet identified are processed in the same way as the enrolment data and the incoming data are compared with the database to see if there is a match. When the comparison is complete, some form of action based on the comparison outcome is generally required. The database search process has been the subject of significant commercial research for other applications and sufficient commercial products are available that this topic need not be discussed further.

The two key areas that distinguish between various biometric systems are: the sensor that measures the human characteristic; and the signal processing that extracts salient features from the sensor output and measures the degree of match between the new subject and known subjects [13]. Data collected by the sensor are processed to extract key features which enable different subjects to be separated from one another by a classifier. This feature extraction process [170] generally results in a significant degree of reduction in the quantity of data, since a large amount of sensor data does not contribute to effective classification. For example, a face recognition processor requires images of the faces of people, where as a typical image from a sensor, say, a TV camera, may include a large amount of information that is not connected with faces and can be discarded. Such informaion may include background information, walls, floor, ceiling, plants etc. [4]. Much other information can be reduced to a symbolic description, e.g. the person has brown hair, and the characteristics of the key eye/nose/mouth geometry may be represented in perhaps a few hundred bytes.

The net result of the data extraction process is generally a compact multi-dimensional data vector which is traditionally called a template when it is enrolled in the database. This data reduction is primarily performed to achieve the separability of subjects, since confusing data is rejected. In addition, a compact description has the advantage of speeding up the process of comparison with the known database. Privacy issues are also aided since the sensor signal generally cannot be reconstructed from the template (this is discussed later). Most feature extractors for biometrics systems are based on some form of Principal Component Analysis (PCA) [10][107], which aims to extract orthogonal data, i.e. independent data in each vector element, on the basis that this will represent the most compact possible description of the input [162]. Other associated work includes the Independent Component Analysis (ICA) algorithm [2], Linear Discriminant Analysis (LDA) [54][171][172] and a memory based approach [147] for which performance increases have been claimed. In addition, Moon and Phillips [109] describe an analysis of PCA algorithms.

Comparison with the known database occurs when an unknown subject must be identified. Data is gathered using the same sensor as was used for enrolment, or one similar, and this data is processed in the same way as the enrolment data. Following salient feature extraction, the incoming data is compared with each template in the database to determine the goodness of match with known data. The match measurement technique may be as simple as the determination of the Euclidian distance between vectors with weighting applied to normalise the magnitudes of the vector elements if required as in (1).

$$M = [k1(A1 - B1)^2 + k2(A2 - B2)^2 + k3(A3 - B3)^2 \ldots] \quad (1)$$

where M is the match measure, kX are the normalising weights and AX, BX... are the elements of the vectors being compared.

Other possible measures may be used [87], but the outcome will always be a number representing the "goodness" of the match between the incoming data and one of the stored templates.

A decision-making process follows the match measurement, whereby the outcome is declared to be either a true match or a non-match. It is also possible to declare that the

result cannot be decided on the basis of the current sample and this outcome may lead to a rejection of the classification attempt or request for a further sample. If a decision is possible, the basic true match/non-match decision may be made by setting a single threshold for the match parameter and declaring that any match result on one side of the threshold refers to a true match and any on the other is a non-match. An appropriate setting for the decision threshold may be determined from the probability density functions for true match and non-match as a function of match value, as illustrated in Figure 2.

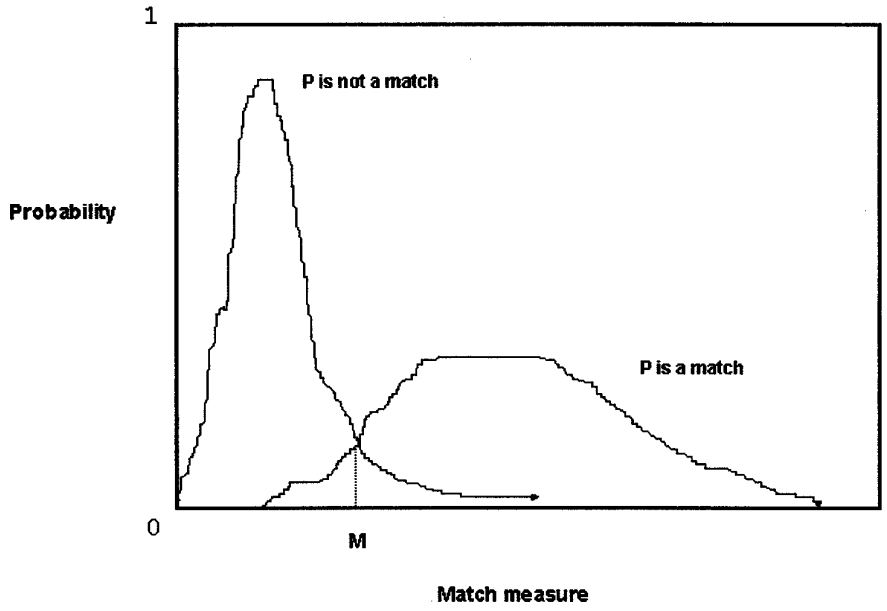

Figure 2: Match Measure

There is value in determining these functions, since they contain the basic performance information on a system, which may be used for system evaluation or for setting thresholds as described below. The two functions may be determined from experimental data as follows. See [160] for a discussion on this topic and for suggestions on further reading.

The true match function can be determined by comparing new data vectors of known persons who are enrolled in the database against their templates in the database. All of these comparisons will be true matches, yielding an indication of the shape of the true match curve. If the database only contains one or a few persons, a number of samples of each could be enrolled and comparison with a number of on-line samples of known people may be used to very roughly estimate the shape of the curve.

The no-match function may be determined by testing the match of as many of the

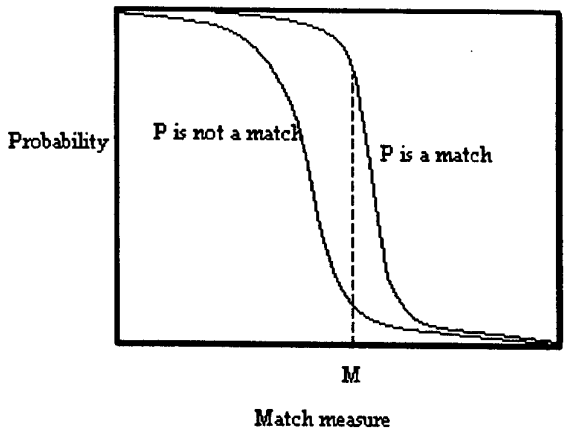

Figure 3: Match measure

templates as possible of people who are not recorded in the database against those who are enrolled in the database. All of these match measures will represent samples of the non-match distribution. The unenrolled test set should be chosen to represent a fair cross-section by race, sex, age etc. of all people who are likely to confront the system, i.e. a cross section of the world population in some systems. If it is not possible to take a sample of this type, the no-match function may be approximated by cross comparison, which involves comparing different people, of all templates of those who are registered in the database, accepting the limitations of the database as a representation of the total population who may confront the system.

Referring to Figure 3, it should be noted that the cumulative probability density functions illustrate a typical situation in biometrics, where there is a significant probability of making a totally unavoidable error. Take for example the situation where the curves have been determined and a new sample has produced the match measure M. For this measured match value there are two possible interpretations:

1. the measure refers to a match
2. the measure refers to a non-match.

Each of these possibilities is a valid interpretation. Which is the right result? If it is declared that the measure shows that there was a match, then there is a finite probability that the decision is wrong and that a non-match occurred. Similarly, if a non-match is declared there is a finite probability that there was actually a match. In either case, there is a finite unavoidable chance of making an error.

It should be noted that unavoidable errors will occur at other match values on either side of M. In general, for any value of match there will be the possibility of finite errors and the decision making process may have one of the following outcomes:
- a true positive declaration - the classifier correctly found a match
- a true negative declaration - the classifier correctly identified that there was no match

– a false positive declaration - the classifier found a match, but the subject was actually not in the database, or the subject was represented in the database, but database entry to which the subject was matched was not the correct one
– a false negative declaration - the classifier decided that the subject was not in the database, whereas he/she actually was represented.

A useful derivation from Figure 2 is gained by integrating the two error regions above and below a range of match values to generate graphs of the cumulative probabilities of each type of error as the match value varies. This results in the Receiver Operating Characteristic (ROC) curve of Figure 4, which conveys sufficient information to allow a decision threshold value T to be set. Any value below T is declared to refer to a match and any above T is declared to be a non-match. The standard Bayesian decision making process calls for T to be set at the Equal Error Rate (EER) where the probability of a false match is the same as the probability of a false non-match. Note that some measures produce high rather than low match values for close matches, but the concepts remain the same. In the real world, the threshold would possibly not be set at the ERR value but rather at some more appropriate setting, depending on the cost of generating an error.

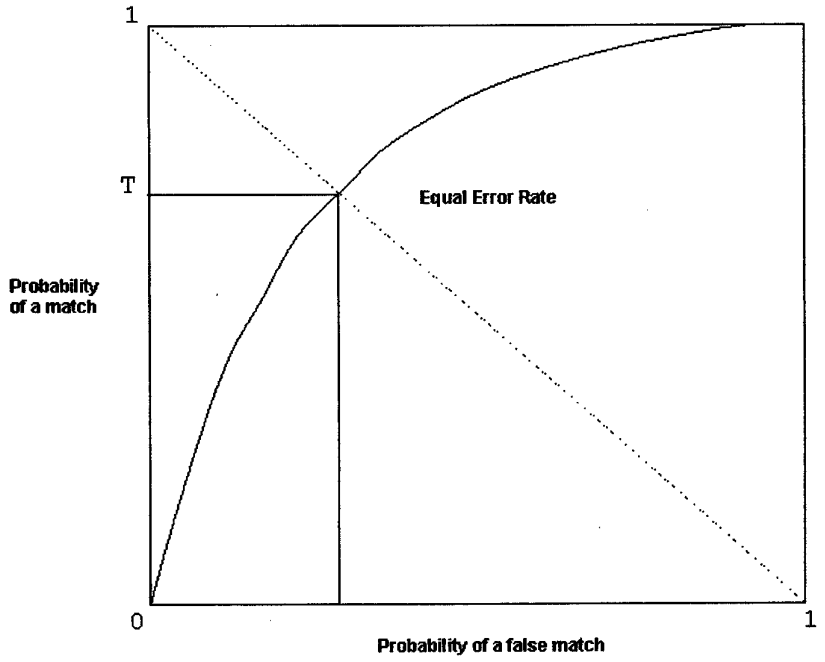

Figure 4: ROC Curve

Thus, the two technology areas that distinguish biometric systems are in the sensor and data collection process and in the signal processing technology. A variety of biometric systems will be discussed with particular reference to these aspects.

3 Biometric Technologies and Applications

3.1 Fingerprints

3.1.1 Sensors

Fingerprints are formed by patterns of raised skin at the tips of fingers. It is thought that the patterns formed are unique [118] to each individual, provided that sufficient features are examined, and sensing the patterns provides effective identification of individuals. A variety of sensors has been applied to the problem of automatically identifying fingerprints. Some examples follow.

3.1.1.1 Capacitive sensors In this technology, the fingertip forms one electrode in a capacitor array. The finger is placed on the dielectric covering of an array of sensing electrodes and high frequency alternating current is coupled into the finger through a separate drive element. The electrical signal capacitively coupled into each sensor element is measured. Where a sensor element is under a raised section of skin, the coupling is greater, since there is no air gap in the capacitor formed with the sensor element. The array element output indicates the proximity of raised skin and a 2D sensor array produces a 2D image representing the skin height of the fingertip. Resolution of the sensors varies, but 500 line pairs per inch appears to be a fairly widely applied standard, it is also the FBI standard, for sensing down to the level of ridge structure. It should be noted that pore structure requires higher resolution. The number of elements may also vary with about 128x128 up to 300x300 being fairly common. The area of fingerprint that is sensed will depend on the size of the sensor, so larger sensors may be needed if high performance is required to ensure that many features are recorded and that successive prints have adequate overlap.

Capacitive sensors are likely to be widely employed in the future since individual sensors are cheap and can be easily interfaced to processing systems.

Despite their advantages, capacitive sensors appear to be relatively delicate in the face of mechanical and electrical abuse. The sensing element array must be covered with a protective layer to guard against wear or scratching, but this layer has a finite life and can be deliberately damaged. ElectroStatic Discharge (ESD) will couple directly into the amplifiers under the array elements, since they are designed to collect electrical energy. The electronics are generally designed to be hardened to ESD, but quoted figures are still relatively low, e.g. 15KV was quoted by Infineon [85]. This may pose problems in high static discharge conditions or when the sensor is deliberately attacked. Capacitive sensors may also have difficulty in sensing fingerprints which are worn or otherwise indistinct, e.g. old people can have poorly defined fingerprints. Approximately 5% of people may be unable to use fingerprint sensors and TEKEY [156] claims that up to an extraordinary 20% of the population cannot use capacitive sensors because of "the dry skin problem". Users may have difficult fingerprints due to wear or poor contrast with conventional sensors. Authentec [8] claims to have a capacitive technology that looks deeper than conventional capacitance sensors. How this works is not made clear in any of the available company literature. Capacitive sensors are also apparently sensitive to dirt or grease, so they may

not be able to operate effectively in dirty environments and some means will possibly be required to keep a regularly used sensor clean, even in clean environments. Overall, capacitive sensors appear to be well suited to applications that call for relatively infrequent use in relatively clean environments and in which very low cost is a necessity. One particular application to which they are uniquely suited is their possible incorporation in future smart cards, removing the need for signature identification [92]. The card will carry a template, a description of the user's fingerprint, and it will also carry the actual sensor which produced it. The card reader will obtain the template from the card and the user will also press a finger onto the card sensor, which will be interrogated by the card reader to provide authentication. Mobile phone activation would also appear to be an application where capacitive sensors could be applied due to their small size and low cost. However, a major question mark remains over how many people cannot use this type of sensor. Available information is not consistent on this critical point.

3.1.1.2 Optical sensors These use a standard 2D TV camera and a prismatic lens system to directly image the fingertip skin pattern [163]. The fingertip is pressed against a flat transparent surface and illuminated obliquely so that total internal reflection occurs where there is no damp contacting skin, but not where there is contact. The pattern of ridges in the skin thus shows up as high contrast bright and dark regions in the TV image. The normal prism-based optical systems introduce foreshortening due to the required oblique viewing, but one manufacturer [56] has developed a holographic optical system that produces an undistorted image. The claimed advantage of optical systems is that the finger is not in contact with the sensing device, only with the optics, which means that ESD and mechanical damage may be less of a problem than with capacitive sensors. The disadvantages are that the optical plate on which the finger is rested must be kept clean to reduce residual fingerprint images, and that the cost is likely to be somewhat higher and the sensor mechanism physically larger than for capacitive sensors. Overall, optical sensors appear to be best suited to high volume, higher performance applications, particularly where a cleaning mechanism can be incorporated.

3.1.1.3 Imaging Infrared ATMEL [6] has developed a linear sensor array of pyroelectric thermal detectors over which the fingertip is scanned in the cross-array direction to produce a 2D array of the fingertip. Minute variations in the skin temperature are sensed to provide a 2D array representing the pattern of ridges in the fingertip. ATMEL claim that the system is very sensitive, even to worn or indistinct fingerprints and the sensors respond to changes in temperature. The biggest problem may be that the finger must be moved to generate signals in the detectors, so the user may need to be relatively skilled in using the system. It may not be as intuitive as simply touching a sensor pad. This is not clear from the information available to date from the manufacturer. The history, current status and future of infrared (IR) technology is discussed in [133].

3.1.1.4 Ultrasonic Ultrascan [161] has developed an ultrasonic scanner to measure the height distribution of skin ridges in the fingertip, forming a 2D array of the ridge pattern. The ultrasonic scanner appears to offer the advantages of insensitivity to ESD, no problems with mechanical damage and possibly a high tolerance to dirt, since the sensor

can "see through" covering materials. The basis for the scanner technology is not clear from the manufacturers information.

3.1.1.5 Mechanical NTT [134] has proposed that an array of tiny mechanical strain gauges may be used to sense the presence of ridges in the fingertip skin. The status of this concept is unknown.

3.1.1.6 Hygiene Hygiene may be an issue in some fingerprint applications, since every user in a sequence must press a finger onto a sensor unit. In addition, most sensor types have no mechanism to distinguish between live and dead tissue, so cadaver or artificial fingerprints may confuse them in the case of a determined effort to circumvent such a sensor. The performance of fingerprint biometric systems is affected by the type of sensor used and Jain et al [89] discuss the relative performance of algorithms when used with either optical or capacitive sensors, with better performance being obtained from optical sensors.

3.1.2 Processing Requirements

Once the 2D image of the fingerprint is obtained by the sensor, it is processed to extract salient descriptors. Many features can be used as the basis for identification, including the following either singly or in combination:
- macroscopic features such as the general pattern type, (e.g. loop, whorl, arch etc.)
- texture features such as ridge direction
- structural irregularities in the ridge pattern such as ridge ending and bifurcations (generally called minutiae) [53][60]
- microscopic features such as pores, which may be detected using high resolution sensors.

Image enhancement is often required to overcome problems with sensing of the ridge pattern. The most commonly used methods appear to be based on the detection and classification of minutiae, often in combination with other processing. The reader is referred to [89] for an example of many of the processes that may be used in a typical fingerprint recognition system.

Of all of the biometric measures, fingerprints appear to be among the easiest to implement and the most practical in a wide range of applications. The sensor technology is relatively straightforward and well developed, the processing load is relatively small and the user requirements are intuitive. Place the finger on the sensor and things happen. A major question mark is the likelihood that many users have fingerprints that are not well enough defined for them to be sensed by some of the currently available sensors [97] and this must be clarified if fingerprint sensors are to be considered for wide use.

Fingerprint-based biometric systems are generally considered to be in the low to medium performance category with claimed EERs in the order of 0.1% or better for typical one-to-one authentication on single finger data. Performance may be improved by using multiple fingers, either in a multi-digit hand scanner or by sequential presentations of fingers. We look at False Acceptance Rate (FAR) and False Rejection Rate (FRR). Some claimed performance data are as follows:

- www.tai-hao.com claim FAR < 1 in 100,000 and FRR < 1 in 1000
- www.ie-oem.com claim FAR < 0.001% and FRR < 0.01%
- www.guardware.com claim FAR < 0.000001 and FRR < 0.0001 or < 0.03 including operator errors
- www.gezmicro.com claim FAR = 0.76% with a 72 byte template, 0.05% with a 90 byte template, 0.009% with a 126 byte template and FRR is sensor determined
- www.biometrica.it/eng/wp_fx3.html claim variable measures, a typical EER of 0.12%
- Jain and Pankanti [87] claim a FAR of 0.07% at a FRR of 7.1%.

Performance can vary widely [81], depending on how it is measured and what equipment is used. Large-scale controlled experiments are required to fully characterise fingerprint sensing technology in a real world environment, as is proposed for FVC2002 [105]. There is also literature that examines the algorithmic view of fingerprint recognition [142].

3.2 Face Recognition

Face recognition is based on the automation of processes to identify a person on the basis of his or her appearance [3]. One of the most well-known investigations into face recognition processing was undertaken by the US Army Research Laboratory. Two significant results from this study were the FERET face recognition algorithm and the FERET facial recognition database [25][26][125][126]. Important research in the area of evaluation and testing of the FR systems was published in [19][20][21][63].

The initial step in any face recognition system is face detection [83], which is a substantial study in itself [79]. Face detection involves localising and extracting the face region from the background. To rephrase the sentence, it means where is the face in the picture rather than who does the face belong to. Face recognition is appealing because it is totally passive and transparent to users. They need not be aware that it is in operation, on the other hand the whole issue of surveillance in public places offends some people. Face recognition is the only current technology that could conceivably be used to search for subjects of interest in moving crowds [131] without disrupting the process, e.g. in an airport.

Some of the issues that arise with the various possible applications of face recognition are:

- The source camera may be different from the test camera, e.g. where newspaper photos are used to enrol a person and that person is then detected in the signal from a TV camera. This requires flexible software.

- Illumination may be variable and uncontrollable [1][31][38][43]. This is particularly an issue outside or in crowd scenes, which rely on natural lighting [56][70][71][98][140].

- The pose of people may be uncontrolled, e.g. in a crowd [69], so systems must be tolerant of pose [102] and distance change [59][68][72][148].

- The background may be intrusive in scenes containing complex structures, e.g. in a street scene.

- Scenes may contain more than one face to be processed [14]. This requires a fast software algorithm.

– Apparent face structures may change with age, health and makeup [95][140].

– Facial adornments such a sunglasses, spectacles or facial hair may change the apparent image, either by accident or design [155].

Despite all of the possible problems, face recognition has been shown to work quite effectively in some applications and it should eventually be relatively low-cost to implement. Related work has also been undertaken on recognising familiar and unfamiliar faces [33]. This is a field that has had little focus and can be illustrated with the following example. People are more familiar with their own cultural or ethnic "masks" and find it easier to recognise one of their own kind rather than one belonging to an unfamiliar cultural or ethnic group. A native from Kenya may find it easier to differentiate one Kenyan face from another, rather than one Chinese face from another if the Kenyan native is unfamiliar with Chinese faces.

3.2.1 Sensors

Sensors for face recognition must provide at least a 2D map of the structure of the subject's face, although some of the evolving high performance systems use a 3D representation of faces [113]. Sources of 2D images include Close Circuit TV cameras [36][114], still cameras, photographs from various sources such as newspapers and passports and drawn images where no photo representation is available. Some of the less widely used imaging technologies such as IR cameras [97] or ultrasonic imagers may be useful, but have not been mentioned in any detail in readily available information. In any event, conventional sources of imagery are readily available, well accepted as part of normal life and relatively low cost, e.g. security cameras.

3.2.2 Processing

Almost all of the characteristics of face recognition systems currently in development are defined by the software rather than the sensor. Two of the main approaches are based on either algorithmic techniques [41][91][99][103][139][150] or neural network learning [35][58][90][93][94][96][101][173][174]. A survey of algorithms used in face recognition can be found at [12]. A statistical model has been used by Edwards et al [50], signal processing has been employed by Podilchuk and Zhang [128] and another approach is outlined by Image Metrics PLC [86]. It appears to be based on a very fast model matching process that is claimed to need no tuning parameters. A summary of technologies that may be utilised in face recognition software can be found in Zhao et al [175] and some algorithm comparisons have been reviewed by Sutherland et al [152].

The basic processes in either algorithmic or learning methodologies are likely to be as follows:

– Find the faces in the scene [79]. This is not a trivial operation and is one of the key problems in face recognition software [39][77]. Techniques used include looking for blob-like regions with consistent brightness and colour of the right size and ovality, looking for blobs with appropriate internal structure, looking for blobs with motion or training a neural network on a wide variety of faces. Objects that are not sufficiently "face-like" will

often be rejected although partial distortion algorithms have been used in experimental work [46].

– Normalise the face images. This may include correcting each face for pose distortion, normalising to a standard size and normalising the intensity/colour content.

– Identify the eyes. The eyes are generally used as the fiducial points in all following operations so their identification and exact location is essential. Most products allow for manual fine-tuning of eye location in the enrolment phase to minimise errors in the database. Manual adjustment is generally not available in automated operation.

– Measure the face geometry and convert it to a compact vector. Most algorithmic methods rely on the concept of eigenfaces [175], where a form of PCA is used to generate an almost orthogonal basis set of face primitives. The vector components result from the correlation of the unknown face with each of the eigenfaces. At least one developer uses the related technique of Local Feature Analysis [122] and some developers use neural networks [157] to generate the classification vectors. The nature of the transformation is not explicit in this approach.

– A template database search and possibly face retrieval for close matches.

This type of processing [123] generally requires significant processing power, due to the complexity of the scene that must be processed. In addition, there are many stages at which human setting of parameters is required, e.g. lighting, decision thresholds etc., so that trained operators are generally required to obtain the best results from current systems. In general, the complexity of the software, the requirement for relatively high computing power and the need for an expert operator means that face recognition is currently a relatively costly approach, although it may eventually become more cost effective as the technology advances. However, even now there are niche applications for face recognition, such as crowd surveillance, in which no other system can operate.

3.2.3 Performance

Face recognition performance has been shown to produce EERs of around 2% in relatively controlled conditions [25]. Data from a crowd surveillance trial in an airport showed typical detection rates for people of interest of around 25% for false alarm rates of around 50 per hour in a high use environment. These results are not particularly encouraging, but they may be better than the results that any other process can currently provide. IR facial scanning, a technology from the late 1990s that claimed to be highly effective, seems to have disappeared below the research horizon [97]. The following references relate to a number of studies that have attempted to evaluate biometric systems [16][40][124].

Processing speed is an issue and none of the systems currently available claim to be able to process more than a few faces per second, which may be a limiting factor in crowd flow scenarios. Speeding up processing can cause problems as well, since individuals may then be processed a number of times, raising the false classification rate and diluting true classifications. In fact, managing the initial face detection problem to optimise input to the classifier is a major issue for face recognition software.

3.3 Hand Dimension, Palm Pattern and Vein Pattern

A variety of technologies has developed around the structure of the hand. The simplest is based on the measurement of a few critical dimensions of the hand when it is placed over aligning pins and imaged by a TV camera, e.g. BioMet Partners Inc [16] who claims a 3D capability. The exact measures used are proprietary information, but measures are likely to include width and length of one or more fingers. This technology is not claimed to be highly accurate, but it is quick and relatively easy to use. It is best suited for authentication to prevent casual false claims of identity and is currently in use at Disney facilities in Florida [100]. Performance data is not available at time of print.

The human handprint related to the fingerprint has been investigated by Jain et al [48]. Moderate levels of performance of around 5% EER are reported and the use of this technology as an adjunct to fingerprint recognition is suggested.

A number of developers have technology based on the scanning of vein patterns in the back of the hand or the palm using short wave IR to provide an image of blood vessels beneath the skin. The basis of the technologies is not known beyond the sensing method, but presumably they use similar decision-making processes to those of other technologies. High levels of performance are claimed for the vein sensing techniques with Veinid [45] claiming "0.0000%" FAR (accuracy up to 4 decimal places).

3.4 Iris

Every iris is thought to have a unique pattern and a few companies exploit this feature by imaging eyes and generating templates based on the iris structure [164][165]. The nature of the template production process is proprietary information, but it is possibly based on a radial sampling technique to overcome scale and pose issues [42].

The imaging process may be a significant problem, since the eye is a small object and to obtain high quality images it must be imaged either with a long focal length system or from a short distance. This will require location of the eyes at a precise point. This may require either bending to adjust height or moving a travelling camera closer to the eye. In any case, the technology will probably require either a very sophisticated tracking system in the sensor or a degree of user skill and acceptance in approaching the sensor. Performance is claimed to be very high, with a EER of 1 in 1.2 million [44]. A discussion on the focus of attention that is based on gaze and sound can be found in [151].

3.5 Retina

The pattern of veins on the surface of each retina is thought to be unique and is used to identify individuals in high-performance biometric systems [136]. The sensor illuminates the retina with low level light and the retina pattern is imaged by a TV camera. The eye must be relatively close to the sensor and aligned properly for this to be possible. The need for a user to submit to illumination of the eye, even if near IR is used, combined with a need to position the head with quite high precision means that this type of system will be best suited to applications in which the users are trained and accepting of the system.

It would not be suited for applications that involved the general public. One possible approach to the generation of retina data is as follows:

– Locate the optic nerve region, a distinctive oval region in the retina.

– Perform a scan around the optic nerve perimeter or some related circular scan, and filter the signal to produce a binary representation of the vein structure. The pattern of veins as a function of angle, which can be likened to a barcode, becomes the data vector, which is then processed as for other biometrics.

Exceptional performance is claimed for this type of system and it is generally regarded as the most reliable of all current biometric measures. However, its use is likely to be limited to very high security applications involving motivated and skilled users, since it is relatively invasive. The strengths and weaknesses are discussed in [135].

3.6 Voice pattern

Voice recognition software has been developed as an input tool for computing systems, where the software translates spoken words into a written representation [111]. This technology can also be used to recognise a speaker's identity, since the voice information is transformed into a symbolic representation that can be used to distinguish between speakers. Voice input products generally have a learning function that shapes the software to provide peak performance for a specific speaker. Much of the underlying software should be readily applicable to voice recognition for biometric applications. The input sensors required for voice recognition are widely used telephone handsets or microphones attached to computer systems. Both are already widely used and familiar to the public, so there are no issues of acceptability and there will be little sensor cost in implementing such systems.

There are many ways in which a voice pattern may be recognised, including algorithmic and learning approaches, but the "standard' method is based on the following type of process [176]:

– Sample power spectrum of the voice waveform at short intervals and over a narrow time window (e.g. $30ms$ overlapping windows every $10ms$).

– Perform a Fourier transform on each sample.

– Take the log of the power spectrum of each sample to normalise for variations in level.

– Perform an inverse transform on the log power spectrum, e.g. Fourier or Cosine, for each sample.

– Select appropriate components of the transform output to use as elements representing that sample window. Components are chosen to minimise transmission channel effects, e.g. phone line or microphone.

– Develop a classification vector, or template, by stacking together the processed elements from a sequence of samples.

The above process will yield normalised templates that are largely independent of the quality of the transmission channel and identification can be performed by requiring all

users to recite fixed sequences of utterances for enrolment and processing, e.g. a sequence of numbers.

The performance of voice recognition systems may be in the region of 1% EER [15] when using a broad range of possible speakers. Data does not appear to be available on the sensitivity of the process to mimics, people who can deliberately change their speaking to match that of others. Since humans may be confused by mimics, it is suggested that voice recognition systems may be also, which would limit their applicability in situations where there was a concerted attempt to pervert their action. In addition, voices may change with stress and state of health. However, it would appear that voice recognition would be very useful in situations where it was not the only security system in use or where there would be a low likelihood of a concerted attack on it. The low cost of the technology and the ready availability and acceptability of sensors must argue in favour of its application in a variety of areas.

3.7 Signature

Written signatures have been used for centuries to verify the identity of the signatory on written documents. However, the recent transfer of documents to electronic form has changed the requirements to verify document authorship. Technologies have been developed to electronically read signatures for verifying the authenticity of electronic documents and mail. The identification of manual signatures on cheques is also proposed. An overview of the technology is to be found in Srihari and Srihari [149]. Jain et al [88] investigated the performance of such a system and found a level of about 2-3% EER. They also found that forgery was successful at confusing such a system. The input devices for signature recognition are generally tablets or stylus systems and cameras or scanners could be used to input manual signatures on cheques.

Unlike the traditional signature on paper, which is subject to forgery, electronic signature and authority recognition systems perform a checking process based on the signature image and include in the processing the characteristics of a person's signature. Even those characteristics invisible at the time of writing, such as the pen's pressure on paper, speed of signing and the slope of letters are used in the checking process.

Electronic signature recognition can handle signatures scanned from paper and extracted from a document or from other digitalizing devices such as pen pads. Advantages of the traditional signature over passwords, for example, are that a person does not forget their signature, does not give it away inadvertently to another person and is fully acquainted with it.

3.8 Keystroke

Keystroke filtering is a behavioural biometric that samples how a password is typed on a keyboard. Essentially, the timing between the keystrokes is measured and then compared against a previous known attempt (template). The keyboard filtering biometric is proved successful when the password is recognisable by the subject, however with a randomly chosen combination of alpha-numeric characters, the biometric is of limited

benefit [168]. One advantage of this system over other biometric systems is that it is cheap to implement and does not require any additional hardware to sample the biometric. It could be suggested that the level of security is only marginally increased due to the ability of another subject to "learn" the password timing, i.e. it would be relatively easy to "beat the system" if the subject was aware of the process.

3.9 Ear

Ear biometrics were developed in 1949 by A Iannearelli [32] and are based upon a 12 measurement point system. In recent times computers have been used to measure these points from a 300x500 pixel image presented to the software. This form of ear biometric detection is susceptible to lighting changes as well as temporal effects. The primary drawback for use as part of a surveillance system is the image resolution required and the inability of the system to work when the ear is obscured by hair. Ear jewellery was not mentioned in the texts examined, but it is likely to reduce the efficiency of the system.

3.10 Chemical (smell)

The human body is made up of around thirty chemical components in various proportions [49]. It is possible to detect these through chemical analysis and to use the results as a biometric identifier. There are limited studies in this area, but the thought is that the analysis could be complex and could not be done in real time [49].

3.11 DNA

DNA is one of the ultimate identifiers of a human being, since it can operate on very small samples of a person's anatomy. The technology is not currently real time, but, should it ever be developed to this level, it could add significantly to the armoury of biometric users [158].

3.12 Work Dynamics and Behavioural Patterns

Each person performs work tasks in a relatively consistent way. For example, the author is typing this manuscript at a relatively slow rate and with consistently recurring typing errors. It would be immediately apparent to an observer if a trained touch typist were to take over the duty, since the speed and accuracy would increase. In addition, the choice of words and the average sentence structure would probably be different. This individuality in performing tasks can provide a biometric measure that identifies an individual and is most suited for use as a secondary and confirming authentication measure that ensures that only an authorised person continues to perform a task after the initial authentication. Measures of timing, order, error rates etc. are likely to be readily available from the computers that interface to many activities, so this type of biometric process

should be relatively easy to apply to a wide range of activities at low cost and without any visibility to the user.

Limitations to this type of technology may include subject variability due to mood, tiredness etc. and the possibility that the characteristics of another person could be mimicked with appropriate training. Despite these limitations, the technology is particularly appealing as a confirmatory measure, since it provides continuing authentication in a manner that is transparent to the user. The input data, such as timing, error rates, structure, etc. as required for the classification process is likely to be readily available from embedded computers in many activities, so the cost is also likely to be low.

3.13 Future Directions

3.13.1 Smart Cards, ID Cards and Passports

Fingerprint sensors are being developed that can be incorporated into smart ID cards [92]. The card will carry a template of the valid user's fingerprint. When plugged into an appropriate reader, the card will provide the template and the current biometric result for processing by the card reader. Thus there is no requirement for centralised or local storage of data and the sensor will be the same as that which was used to generate the template. This type of system will therefore, be scalable to large numbers of users, practically without limit, while retaining a relatively high degree of security and speed of operation. The biometric smart card approach will be applicable to a wide variety of uses, including Point of Sale (POS) cards, ID/license cards and passports. It would be valuable to investigate the possibilities of this type of approach with other sensor types.

3.13.2 Combined Systems

Many of the systems currently in the marketplace have been developed around a single biometric method, whereas there may be merit in combining two or more measures to overcome limitations of individual technologies [61][78]. For example, a combination of voice and face recognition technologies [37] may be competitive in performance with high-end fingerprint or vein detection technology, but use readily available sensors. Some work has been done in the field of combined sensors [80], but more may be valuable. In addition, most current work appears to be focused on higher performance technologies, whereas there may be value in combining technologies that are less efficient by themselves in producing functional systems [84]. For example, a simple sorting system based on sex, 1 in 2, height, perhaps grouping to 1 in 5, and skin colour, perhaps 1 in 3, could sort to around 3 in 100, which is comparable with some recognised low-end biometric systems. Simple information of this type is often ignored in systems design, whereas it could probably greatly enhance performance at little cost. There was a lot of discussion on this issue on the recent biometrics conference (see [17]), generally concluding that regardless of the fact that combined systems should provide better results there is no successful implementation of it up to date. The main problem is seen to be how to combine different measures.

Table 1: Biometrics comparisons summary

Biometric	Finger	Face	Hand	Iris	Retina	Voice	Signature	Keystroke	Ear	DNA
Access control	Y	Y	Y	Y	Y	Y	Y	Y	Y	N
Surveillance	N	Y	N	N	N	Y	N	N	Y?	N
Accuracy	very high	high	high	very high	very high	med	med	low	?	very high
Reliability	high	med	med	high	high	low	low	low	low	high
Error rate	1 in 500+	no data	1 in 500	1 in 131,000	1 in 10 mil	1 in 50	1 in 50	no data	?	no data
Errors	dryness, dirt, age	light, age, glasses, hair	hand injury, age	poor light, contact	glasses, contact lenses	noise, cold weather	alter style	hand injury, tired	light, hair	none
False positives	highly unlikely	unlikely	very unlikely	very unlikely	highly unlikely	likely	likely	unlikely	?	highly unlikely
False negatives	highly unlikely	very likely	likely	very unlikely	highly unlikely	very likely	very likely	very likely	?	highly unlikely
Security	high	med	med	high	high	med	med	med	?	high
Stability	high	med	med	high	high	med	med	low	?	high
User acceptance	med	med	med	med	med	high	high	high	?	low
Intrusiveness	med	low	low	low	very high	low	low	low	low	high
Ease of use	high	med	high	med	med	high	high	high	med	low
Low cost	Y	Y	N	N	N	Y	Y	Y	Y	N
Standards	Y	?	?	?	?	?	?	?	?	Y
Strengths	existing databases in operation	surveillance, checkable by humans, can use existing equipment		high accuracy	accuracy	low cost, can be used for surveillance	low cost	low cost, no additional hardware required	profile imaging possible, surveillance use	accuracy
Weaknesses	public acceptance, environment -ally affected, specialised hardware	environment-ally affected, biometric changes	environment-ally affected, biometric changes, specialised hardware	public acceptance, glasses, specialised hardware	public acceptance, glasses, specialised hardware	accuracy	accuracy	accuracy	environ-mentally affected	not real-time, expensive, specialised operations, specialised hardware

3.14 Summary

We provide here description of the variables used in our summary table (see Table 1). The data for the comparison chart is sourced from the National Center for State Courts [112], organisation that serves the US court system by providing up-to-date information and hands-on assistance through original research, consulting services, publications and educational programs.

Table 1 represents the major focal areas of biometrics research, as follows: fingerprint, face, iris, retina, voice, signature, keystroke, ear and DNA. The dimensions used to rate each used to rate each biometric focal area describes categories of application usefulness. The scales used in each dimension evaluate each category in relation to the set of all categories used in this comparison.

- Verification - Whether or not the Biometric is capable of verification. Verification is the process where an input is compared to specific data previously recorded from the user to see if the person is who they claim to be.
- Identification - Whether or not the Biometric is capable of identification. Identification is the process where an input is compared to a large data set previously recorded from many people to see which person the user is.
- Accuracy - How well the Biometric is able to tell individuals apart. This is partially determined by the amount of information gathered as well as the number of possible different data results.
- Reliability - How dependable the Biometric is for recognition purposes.
- Error rate - This is calculated as the crossing point when graphed of false positives and false negatives created using this Biometric.
- Errors - Typical causes of errors for this Biometric.
- False Positive - When a test incorrectly gives a positive result (someone is able to impersonate someone else) where 5-highly unlikely, 4-very unlikely, 3-unlikely, 2-likely, 1-very likely.
- False Negative - When a test incorrectly gives a negative result (someone is able to avoid identification as self) where 5-highly unlikely, 4-very unlikely, 3-unlikely, 2-likely, 1-very likely.
- Security level- The highest level of security that this Biometric is capable of working at.
- Long term stability - How well this Biometric continues to work without data updates over long periods of time.
- User Acceptance - How willing the public is to use this Biometric.
- Intrusiveness - How much the Biometric is considered to invade one's privacy or require interaction by the user.

- Ease of Use - How easy this Biometric is for both the user and the personnel involved.
- Low cost - Whether or not there is a low-cost option for this Biometric to be used.
- Standards - Whether or not standards exist for this Biometric.

4 Applications

The following proposals have been mentioned in the literature and we consider this discussion an attempt to identify possible applications for biometric technology purely on the basis of the technical feasibility. There are many unknowns in the current technology and rapid advances are being made in other areas, so this summary may be incomplete or based on conjecture in some areas. Despite possible shortcomings, it is presented as an attempt to identify areas where it may be worthwhile to investigate further in view of the wide scope of possible applications or the significance of individual ones.

4.1 Computer Systems

Most computers already have voice input through a sound processor and low cost fingerprint sensors are readily available as peripherals. Handwriting can be input via stylus pads, and face data and possibly iris data can be obtained via relatively low cost cameras. Work patterns should be easily sensed through keyboard usage.

Some key areas in which biometrics could be applied to computer systems include:

– Log-on verification, removing the need for passwords. The primary sensor is likely to be fingerprint [75], although signature, face, voice or combinations could also be used. In situations requiring extreme security, additional sensors may be justified and vein, iris or even retina scanning could be considered.

– Continuing verification throughout a session could be carried out in the background by work-pattern sensing, or by fingerprint, signature, face or voice on request to ensure that the person who originally logged in is still the current user [47].

– E-mail or other document source verification and access control could be carried out by signature, fingerprint, voice or face, e.g. to authenticate that a document truly originated from a particular person. Combinations could be considered and, in situations requiring higher security, vein, iris or retina scanning could be considered, although these might be better used to screen users during log-on.

– Encryption for secure data transmission could include biometric authentication [78]. Relatively high performance levels would be required, possibly needing high quality fingerprint, vein, iris or retina based systems.

Overall, fingerprint verification of user IDs appears to be the single most likely large-scale application in computing in the near term along with face and voice recognition after further development of these technologies (see [24] [40]).

4.2 Access Control

In low security areas, voice authentication could be convenient for users along with fingerprint access in environments where the sensor could be protected from physical damage. Face recognition could be considered in well lit areas [64][65][82]. Hand geometry and vein pattern would also appear to be suitable.

In high security areas, high end fingerprint or vein identification may be suitable, but iris and retinal scanning may be required. Combinations of lower performance sensors may also yield suitable performance [34].

House security would require relatively low cost systems and fingerprint locks may be suitable. Voice may be subject to mimicry and lighting may be difficult to control for face recognition. Hand and vein print sensors may be at risk of environmental damage and insect contamination.

Other work discusses access through borders, drug control [28] and airports [55] and there is also a reference to biometrics in the Correctional Services [27].

4.3 Staff and Client Management

Time-keeping could be implemented using fingerprint technology [53]. Face and voice recognition [67] may be convenient and fast for small staff numbers, but voice could possibly be confused by a mimic. Hand shape, where staff numbers are small, or vein print could be functional in controlled environments [48].

Payroll and other payment processes could be managed by fingerprint, vein ID or hand shape analysis for small numbers of staff. Iris recognition may be worthwhile with very large staff numbers [81].

Reduction of social security fraud may need a high quality biometric technology because individuals must be identified from a large number of participants. High-quality fingerprint or vein ID would appear to be best suited from ease of use considerations, although iris may also be acceptable. Lower performance technologies such as face, voice or signature may be used in combination. Retinal scanning may be too intrusive to be widely accepted.

Staff training requirements and progress could be monitored using a relatively low level system such a fingerprint, voice, face or signature in combination with other ID recognition systems.

Movement and deployment of military groups or other functional groups could be managed using a combination of conventional ID technologies and a low performance biometric measure to authenticate IDs [121].

4.4 Purchasing and Commerce

ID over a phone connection for transaction verification could be provided by voice recognition.

Credit card use could be verified by a stored biometric template. Fingerprint analysis appears to be the most useful because the sensor can be incorporated into the card. However, signature validation is already used and could be readily automated. Face recognition could be effective and non-intrusive, using automatic comparison of card photo and presented face, but it will require additional sensors and a high level of standardisation.

Cheque verification is currently provided by signature cross checking, a process that could be automated.

Complex purchase sequencing, such as buying an airline ticket, paying insurance and taxes, boarding an aircraft, transferring flights and disembarking with luggage collection could be automated using lower performance biometrics such as face recognition or fingerprint, signature or voice analysis to verify identities along the way. Higher performance iris ID verification is being trialled in this way in an airline passenger management system [57].

Web commerce is growing but security could be enhanced if biometric authentication of a user's identity was available, particularly for credit card transactions [119]. This would require widely available sensors and voice would appear to best fit that requirement. If fingerprint sensors become widely available on PCs, they may be useful in this role, as would face recognition if cameras became widely available.

4.5 Automotive

Any biometric sensor [82] that protects a motor vehicle will be subjected to a wide range of environmental hazards (rain, heat, electrostatics etc.). It will also be subjected to tampering and yet will need to be reliable for the life of the vehicle. At this stage, it does not appear that any biometric technology can meet this requirement alone, but it may be possible to add a fingerprint sensor to the key to verify ownership. Once the owner is in the vehicle, their voice or fingerprint may be used to adjust preferences such a seat height, air conditioning etc. Auto theft could be reduced if the engine management system would only start the motor when a genuine user was identified via a fingerprint or voice signature. Biometrics such as voice or fingerprint could also be used to determine the ID of the driver in the event of an accident or traffic infringement although this raises issues of privacy and civil liberties [78].

4.6 Crowd Management

Large groups of people pass by customs desks and are identified primarily on the basis of their facial features compared to their photographs. This process could be automated with face recognition software (see [63]) and alternative biometrics such as signature verification and fingerprint, vein or hand dimension recognition could also possibly be used to verify that the user of the passport is the person to whom it was issued. In addition, casual border crossings, in normal commercial activities for example, could be managed using biometrics such as hand dimension, face or fingerprint verification to track regular users.

Sporting and entertainment fixtures accommodate tens of thousands of people. All of these people need to be checked to determine that they have valid access on entry and

to specific areas in the facility. If patrons can be enrolled into a biometric system off-line while booking, the validity of tickets can be checked automatically at the venue. Hand shape is being used successfully in this role [100] and other easy-to-use technologies such as face recognition may also have application.

Crowd surveillance is particularly difficult where a large number of people must be scanned to detect one or a few people of interest. Face recognition is the only biometric that may be applied in this way, since it can scan large numbers quickly and without their active participation.

4.7 Regulating Equipment

Theft of equipment of any type may be discouraged if the equipment is protected by a biometric system that will not allow it to be operated by unauthorised users. Anything from a mobile phone to a road-building machine could be protected. Appropriate biometrics would include the lower performance low-cost systems such as fingerprint, voice or face recognition. Particularly important or large equipment could be protected by higher cost biometrics such as vein ID or iris verification.

In the military field [47], activation or de-activation of weaponry could be controlled by biometrics. Nuclear weapons are apparently currently controlled by complex key and password controls; high quality biometrics, such as iris or retina scanning could also possibly be used to validate the authority of commanders in charge of such weapons. Other high value weapons, e.g. artillery, could possibly be protected by biometric systems to ensure that they could not be used by enemy forces if captured. Landmines, individually or in clusters, might also be protected by biometric security devices to ensure that they could only be activated and de-activated by qualified engineers. Whatever systems were contemplated in the military environment would need to be physically robust and most low value weapons systems may be better left unprotected, since there could be advantage in being able to use any available weapon in battle.

4.8 Medical

Access to high value or narcotic drugs could be controlled through low performance biometric identification systems used in conjunction with other ID verification measures to control access to and to track usage. Sensors would need to be widely dispersed, so only low cost unobtrusive devices would probably be suitable. Fingerprint, signature or voice verification would appear to be the most likely candidates [82].

Patients in the medical system must be identified before surgical procedures and for drug usage. Fingerprint recognition may be the most suitable biometric for this use in conjunction with other ID verification systems, since most other measures are likely to be relatively unstable in the face of medical procedures, e.g. speech may be slurred or a signature could be erratic under drug use [93].

4.9 Education

Simple logon to the school computer system using fingerprint [75] or verification of the identity of students attending exams to guard against cheats may be possible using lower performance biometrics, such as hand dimension, face or fingerprint. Stress may rule out signature or voice recognition.

Entry to school buildings may be controlled using biometrics that are invariant to age, as students physical characteristics may change throughout the space of a year. Fingerprints may be the most effective solution to this problem.

5 Associated Issues

5.1 System Testing

It is essential that a biometric system is characterised in a manner that is meaningful and trusted by potential users. It is always easy to slant results by choosing test data that favours a particular system and by fine tuning it for best performance against a specific data set. It should also be recognised that there are two classes of testing, one based on the underlying technology and the other based on real world usability. This is important because the final usability of a system may depend only marginally on its technical capability and a system purchased purely for technical excellence could be disappointing. Conversely, a system may have superior performance for the time being, because it is well refined, but the comparative success of that system may inhibit research on much more technically capable competing technologies that may ultimately be more successful, but which do not yet have refined, experimental environments.

Phillips et al [124] propose a multi-phase testing regime that provides for technology testing, controlled scenario testing and uncontrolled real world testing. This approach incorporates both types of testing and should overcome the problems identified above. In addition, Phillips identifies some of the key test issues involved in the purchase decision, including the need to keep vendors fully aware to ensure that spurious decisions do not work unfairly against any particular system. The Phillips methodology was successfully employed in the FRVT2000 facial recognition vendor test [125][154].

Any testing methodology will require trusted test data that can be used to refine performance through system development and then used to test the system in the lab.

Key data capture requirements for a standard database are detailed below.
- The requirements must be taken with sensors representative of those to be used in any final system.
- The people must represent a cross section of likely users in biometric type and likelihood of presentation.
- They must be divided into at least two sections: one for development and initial testing and the other for blind testing, i.e. testing systems on data that they have not yet been exposed to.
- There should be sufficient data to generate meaningful statistics. An appropriate size is difficult to determine [160], but generally large databases are preferred. A rule of thumb

is to test until at least 30 errors have been recorded [160], which allows some degree of confidence in the results. This will obviously require massive, expensive testing for higher performance systems where errors are unlikely. It is interesting to note that one of the major users of biometrics recently reported, "We will not spend big dollars on testing. Quick tests generate enough information to 'fish or cut bait' "[100], implying that large scale testing, although statistically necessary, may not be essential for real world decisions.
- If possible the data should be gathered in a form that will allow many types of application areas to be examined, not just one specific application, e.g. fingerprint data could be gathered using a variety of sensors without much additional cost when compared to using just one type of sensor.
- The data should be gathered using a published and accepted methodology and with a mechanism to enable users to add data in a controlled manner.

Standard test databases have been developed for a range of biometrics and links to many are available at www.biometrics.com.

Test results are often used to compare systems or technologies, so a presentation that shows underlying performance of the algorithm may be preferred. This would ideally take the form of the probability density functions for true match and true non-match, or the equivalent error curves, as functions of the match metric. An alternative would be the ROC curve and the EER may also be quoted as a quick assessment result. Reject rates or missed opportunity rates should also be quoted. Many biometric systems incorporate software that rejects poorly gathered data from the classification process and some may have trouble processing data fast enough to keep up with the data stream. These effects should be quantified and quoted in the results. Associated data should include the identification of data sets used for testing, along with a description of their make-up and examples of raw data used.

Where a system is used in a mode that generates an alarm, the threshold setting for the alarm should be quoted and the method by which the threshold was derived should be noted.

A natural question that arises when undertaking performance testing relates to the level of performance required. It is often the case that performance can be tailored to an application by choosing an appropriate level of sensor or processing sophistication. For example, GEZ Microsystems [66] quotes a variety of false acceptance rates for their fingerprint recognition technology that varies by very large amounts depending on chosen template size. This ranges from FAR of 0.76% at 72 bytes to 0.009% at 126 bytes. Any testing process [106] must attempt to tailor systems under test to obtain representative results in a chosen application following a standard that allows comparison with other systems. In addition, determining the required level of performance for applications appears to be one area that has not been the subject of much research. Most of the work in biometrics to date has been devoted to developing the technology and there appears to be a significant requirement for operational research to quantify performance levels and trade-off costs in a variety of applications [24].

5.2 Human Rights, Freedom and Legal Issues

There is a perception on rights in a free society regarding the privacy and anonymity, and concern on possible misuse of it. Biometrics systems appear to shift the privacy balance by allowing authorities to rapidly and reliably identify individuals, possibly without their knowledge that it has been done. This increase in the ability of the State to track citizens will have positive implications since it will hinder criminal activity. However, there are many members of society who object on philosophical or religious grounds to State knowledge of their activities. As a result of the general desire for privacy and anonymity, democracies generally have laws that protect the privacy of citizens and any biometric system will need to comply with these laws. Further comments reflecting race issues are discussed in [104].

RAND Corporation researchers carried out a survey of the legal and sociological implications of biometric systems [169], in particular how the US Army would need to manage any application of the technology. They concluded that there are no new issues that cannot be handled by existing laws on privacy. Other sociological issues, particularly of a religious nature, will need to be considered in the future if biological systems are to be widely used. Hygiene may be another social issue that works against biometrics in these days of dangerous, transmissible diseases. Contact sensors, such as fingerprint or hand devices, in regular use will build up dirt and could be a source of infection. For this reason, non-contact sensors may be preferred for applications requiring high throughput of the general public. This should not be an issue in one-to-one authentication tasks, particularly those in which the sensor is carried by the user in a smart card.

5.3 Reliability and Security

Reliability will become a major issue if biometrics come into widespread use. For example, if all of a person's day-to-day transactions rely on biometrics to validate their identity, it will be inconvenient if the biometric measurement changes or the system fails and the person is no longer recognised. It seems likely that some biometrics will be so effective at verifying identity that they may in future be relied on as the primary authority and any failure may be difficult to remedy unless there is a formal fail-safe procedure in place.

The reliability of biometric systems may also be deliberately compromised by malevolent operators. Should the technology eventually be very widely used, criminal or terrorist elements may find it profitable to attack the controlling systems either to shut them down or to hijack identities. Thus, although individual security may be enhanced by biometric systems, the options for large scale mischief may be increased, requiring even more stringent control of central systems. Distribution of systems (e.g. via smart cards with embedded sensors) may be one way to mitigate this problem.

Even though biometric systems may increase individual security, the overall effect on the complete environment that the biometric system is operating in should be assessed for vulnerability.

One of the major imponderables with some of the higher performance systems is to estimate the performance in the extremes of the probability distributions. For example, it

is often claimed that no two fingerprints are the same. This is impossible to prove of course, since it is not feasible to sample the fingerprints of every living or deceased person to prove it. Rather, it is accepted that no-one has ever found two fingerprints that match in the history of forensic fingerprint analysis, so it is an article of faith that the contention is true. Similar claims for signature uniqueness are made for technologies such as iris recognition and retinal scanning, again with no way to prove the contention. Further work may be required to estimate bounds on performance for very high performance systems, rather than just assume that the current uniqueness dogma is correct [118].

5.4 Universality

Widespread acceptance of biometric systems will require some degree of standardisation of the systems in use. For example, there would be no point in presenting a passport with face data encoded on it if the country you are entering has a fingerprint reader to verify your identity. This will not be a problem in many applications where the system only needs to function in a closed environment and there may be security advantages in not publicising the nature of the system. However, as soon as users need to access multiple systems or systems need to exchange data, there will be a standardisation problem. Significant effort is being expended to define standardised interfaces etc. to ensure maximum interoperability, but any enterprise contemplating the implementation of biometric systems [121] should at least consider standardisation issues.

5.5 Acceptance

Biometric systems will only be useful when they are accepted by all who must use them [127]. Door access and computer log-in control should pose no problems, since employees will accept the advantages of an automated system in these applications. However, some of the more marginal applications, such as iris scanning for verifying aircraft passenger identity throughout the embarkation, disembarkation and customs activities associated with an airline flight may be seen to be risky to some users. Although biometric systems promise lower operating costs in this type of application, they come at the price of reduced job opportunities and customer unease. Such an application, would need to be tested very carefully before introduction, since if it was not accepted by all users, the resulting hybrid may be more costly in operating expenses and customer dissatisfaction than a fully manual system.

6 Conclusions

Biometric techniques have been widely used in the past with human interpretation of results, e.g. fingerprints and signature recognition. Advances in computing technology have made possible fully automated systems based on past concepts as well as totally new ways of identifying people. The historical acceptability of some techniques, combined with the increasing need to guard against illegal activity suggests that biometrics will be more widely employed in the near future. An additional driver in favour of biometrics is that it is

likely to be more cost effective than current methods in some activities, particularly in the management of password access to secure computing systems and in controlled physical access. Thus, there may be a significant cost driver which may force private industry to take up the technology . In addition, public enterprises such as the military may be forced to take up biometrics to improve efficiency and effectiveness, as well as to lower costs. The drivers that may oppose rapid take-up of the technology could include: disappointment with real world results when compared to manufacturer's claims, problems with managing the security of associated systems, e.g. databases, and problems with legal or civil rights issues that have nothing to do with the technology, but will have significant impact on its use.

In this environment it will be prudent that all interested organisations keep a close watch on developments. Many of the concepts are still new and some are likely to be promoted by their advocates with more than due enthusiasm. There will be a need to maintain vigilance and a sceptical view of claimed performance to ensure that realistic expectations are maintained. This will be aided by the continuing development of rigorous procedures and methodologies for comparative testing. Legal issues will also need to be sorted out when the true capability of some of the technologies become clearer.

Although biometric systems will need to be proved in the harsh light of the real world, user organisations must ensure that they test potential systems [23] in ways that take account of their known and likely shortcomings, rather than subject them to inflexible testing procedures. The technologies are new and developing rapidly and it would be unfortunate for an organisation to prematurely decide that biometric technology is of no use to it. There may well be a good case for either modifying the testing to better match the biometrics capability, or of deciding to wait for further developments in the technology that may better match it to the problem to be solved. This is a technology that may well offer a great deal in the future and interested organisations should remain open minded, but with an underlying level of scepticism.

In summary, fully developed biometric technology is already available for some applications and it is likely to be both efficient and cost effective. Large organisations should develop strategies to assess the current capabilities of technology [18], to predict future trends and to develop plans for implementation should viable applications be identified.

Various information sources are available to keep abreast of developments in the biometrics industry [22].

References

1. Adini, Y. Moses, Y. and Ullman, S. (1997) Face Recognition: The Problem of Compensating for Changes in Illumination Direction, IEEE Transactions on Pattern Analysis and Machine Intelligence, 19 (7) 721-732.

2. Akaho, S. and Umeyama, S. (2001) Multimodal Independent Component Analysis - a Method of Feature Extraction from Multiple Information Sources, Electronics and Communications in Japan, Part 3, 84 (11) 21-28.

3. Akamatsu, S. (1999) Computer Recognition of Human Face A Survey, Systems and Computers in Japan, 30 (10) 76-89.

4. Atherton, T. and Kerbyson, D. (1997) Reducing false alarm rates in surveillance imaging using significance testing, IEE.

5. Atick, J. (2001) Biometrics, Technology Review, Jan-Feb 2001.

6. ATMEL, San Jose, California company, last accessed October 2002, <http://www.atmel.com/atmel/products/prod42.htm>.

7. Attrasoft Inc, Savannah, USA, company web site, last accessed November 2002, <http://www.attrasoft.com/>.

8. AuthenTec Inc, Melbourne, California, company information, last accessed October 2002, <http://www.authentec.com>.

9. AuthenTec, Inc, Melbourne, Florida, (2002) FingerLoc Powers Biometric Authentication For SENSE's Security Applications, press release.

10. Baek, K., Draper, B., Beveridge, J. and She, K. (2002) PCA vs. ICA: A comparison on the FERET data set,. The 6th Joint Conf. on Information Sciences, Durham, North Carolina, 824-827.

11. Baker, S. and Matthews, I. (2001) Equivalence and Efficiency of Image Alignment Algorithms, IEEE Conf. on Computer Vision and Pattern Recognition, 1090-1097.

12. Barrett, W. (1998) A Survey of Face Recognition Algorithms and Testing Results, 31st Asilomar Conference on Signals, Systems & Computers, 1, 301-305.

13. Barton, J., Keenan, J. and Bass, T. (2001) Discrimination of spatial relations and features in faces: Effects of inversion and viewing duration, British Journal of Psychology, 92, 527-549.

14. Biederman, I. and Kalocsai, P. (1997) Neurocomputational Bases of Object and Face Recognition, Philosophical Transactions of the Royal Society London, Biological Sciences, 352, 1203-1219.

15. Bimbot, F., Koolwaaij, J., Hutter, H., Lindberg, J., Jaboulet, C. and Pierrot, J. (2002) An Overview of the CAVE Project Research Activities in Speaker Verification, last accessed October 2002, <http://www.PTT-telecom.nl/cave>.

16. BioMet Partners Inc, Pestalozzistrasse, Switzerland, company web site, last accessed October 2002, <http://www.biomet.ch/>.

17. Biometrics 2002, London, UK, <http://www.biometrics-2002.com>.

18. Biometric Device Protection Profile (BDPP) (2001), UK Government Biometrics Working Group, Draft Issue 0.82.

19. Biometix, Face Recognition Analysis for the CCTV Project, client report, 25 pages.

20. Biometrics Institute, Non-Intrusive Biometric Testing Technology Evaluation, client report, 55 pages.

21. Biometrics Institute, Scenario Testing Report, 25 pages.

22. Biometric Market Intelligence (2000) in Industry Insight and Analysis for the Biometrics Marketplace, published by Acuity Market Intelligence, web site under construction as of October 2002, <www.acuitymi.com>.

23. Biometrics Working Group (2000) Best Practices in Testing Biometric Devices, in Best Practices in Testing and Reporting Performance of Biometric Devices Version 1.0, 1-14.

24. Blackburn, D. (2001) Evaluating Technology Properly - Three Easy Steps to Success, Corrections Today, 63 (1).

25. Blackburn, D., Bone, M. and Philips, P. (2001) FRVT 2000 Evaluation Report, Facial Recognition Vendor Test 2000, DoD/DARPA/NIJ.

26. Blackburn, D., Bone, M. and Phillips P. (2000) FRVT 2000 Evaluation Report Executive Overview, Facial Recognition Vendor Test 2000, DoD Counterdrug Technology Development Program Office.

27. Bone, M. and Crumbacker, C. (2001) Face Recognition, Assessing its Viability in the Corrections Environment, Corrections Today July 2001.

28. Bone, M., Wayman, J. and Blackburn, D. (2001) Evaluating Facial Recognition Technology for Drug Control Applications, ONDCP International Counterdrug Technology Symposium, June 2001.

29. Bow, S. (2002) Pattern Recognition and Image Preprocessing, 2nd edition Marcel Dekker Inc, chapters 8 and 9.

30. Bowman, E. (2000) Everything You Need to Know About Biometrics, Identix Corporation Jan 2000.

31. Bruce, V. (1999) Identification of human faces, IEE Conf. Publication. N 465 II, 615-619.

32. Burge, M., Burger, W. (2000) Ear biometrics in computer vision, Pattern Recognition, Proc. 15th Int. Conf. vol 2 , 822-826.

33. Burton, A. (1997) Recognising familiar and unfamiliar faces, IEE.

34. Busch, C. (2001) Biometric Authentication for Access Control, Sensors in Intelligent Buildings, 2001 Wiley-VCH Verlag GmbH.

35. Carpintero, A., Castellanos, J., Rios, J. and Segovia, J. (1993) Automatic face recognition for access control, Int. Joint Conf. on Neural Networks. IEEE Service Center, Piscataway, NJ, v2, 1289-92.

36. Chellappa, R., Zhou, S. and Li, B. (2002) Bayesian Methods for Face Recognition from Video, Center for Automation Research, University of Maryland, College Park, MD 20742.

37. Chibelushi, C., Mason, J. and Deravi, F. (1997) Integrated person identification using voice and facial features, IEE Colloquium on Image Processing for Security Applications. London, UK, Digest no 1997/074, 4/1-4/5.

38. Choi, J. Lee, S., Lee, C. and Yi, J. (2001) A real-time face recognition system using multiple mean faces and dual mode FisherFaces, IEEE Int. Symposium on Industrial Electronics, 1686-1689.

39. Chua, C. Han, F and Ho, Y. (2000) 3D Human Face Recognition Using Point Signature, 4th IEEE Int. Conf. on Automatic Face and Gesture Recognition, 233-238.

40. Common Methodology for Information Technology Security Evaluation, (2002) Ver 1.0, <http://www.commoncriteria.org/docs/ALC_FLR/alc_flrv11.pdf>.

41. Cruz-Llanas, S., Ortega-Garcia, J., Martinez-Torrico, E. and Gonzalez-Rodriguez, J. (2000) Comparison of Feature Extraction Techniques in Automatic Face Recognition Systems for Security Applications, 34th Int. Carnahan Conf. on Security Technology, 40-46.

42. Daugman, J. (2001) How Iris Recognition Works, University of Cambridge, Cambridge CB2 3QG, U.K.

43. Debevec, P., Hawkins, T., Tchou, C., Duiker, H., Sarokin, W. and Sagar, M. (2000) Acquiring the Reflectance Field of a Human Face, SIGGRAPH 2000, 1-12.

44. Iridian Technologies Inc., developer information, last accessed October 2002 <http://www.iridiantech.com>.

45. Veinid, California, USA, developer information, last accessed October 2002, <http://www.veinId.com>.

46. Ding, R., Su, G. and Lin, X. (2002) Face recognition algorithm using local and global information, Electronic Letters, 38 (8).

47. DoD Biometrics, Frequently Asked Questions, last accessed October 2002, <www.c3i.osd.mil/biometrics>.

48. Duta, N., Jain, A. and Mardia, K. (2002) Matching of palmprints, Pattern Recognition Letters, 23 (4) 477-485.

49. Dysart, A. Biometrics, University of Michigan, Dearborn EECS 598 Term Paper, Winter 1998.

50. Edwards, G., Lanitis, A., Taylor, C. and Cootes, T. (1997) Face recognition using statistical models, IEE Colloquium on Image Processing for Security Applications, London, UK, 2/1-6.

51. Erskine, R. (1988) Naval Enigma: The Breaking of Heimisch and Triton, Intelligence and National Security, v.3 n.1 , 171-172.

52. Espinosa-Duro, V. (2000) Biometric identification system using a radial basis network, 34th Int. Carnahan Conf. on Security Technology, 47-51.

53. Espinosa-Duro, V. (2001) Minutiae detection algorithm for fingerprint recognition, Int. Carnahan Conf. on Security Technology, 264-266.

54. Etemad, K. and Chellappa, R. (1997) Discriminant analysis for recognition of human face images, Optical Society of America, 14 (8) 1724-1733.

55. Evaluating Biometrics for Airport Security, An Overview, (2001) (hard copy available from LOD, DSTO Edinburgh).

56. Exact Identification Corporation, Sacramento, USA, last accessed October 2002, <http://www.aprint.com>.

57. Eye Ticket Corporation, (2002) company web site, <http://www.eyeticket.com/>.

58. Fadzil, M. and Choon, L. (1997) Face Recognition System based on Neural Networks and Fuzzy Logic, ICNN'97 Pattern Recognition and Image Processing, 1638-1643.

59. Fettke, M., Sammut, K., Naylor, M. and He, F. (2002) Evaluation of Motion Detection Techniques for Video Surveillance, Information Decision and Control, 2001 IEEE.

60. Finger-Scan Technology, last accessed October 2002, <http://finger-scan.com/finger-scan_technology.htm>.

61. Frischholz, R. and Dieckmann, U. (2000) BiolD: a multimodal biometric identification system, Computer, IEEE Computer , 33 (2) 64-68.

62. Fukui, K. and Yamaguchi, O. (1998) Facial Feature Point Extraction Method Based on Combination of Shape Extraction and Pattern Matching, IEICE Trans. Systems and Computers in Japan, 29 (6) 2170-2177.

63. Gaertner, PS et al., "Identifying a Face in a Crowd: A report on the trial of one-to-many facial recognition systems at Sydney Kingsford Smith Airport", Draft DSTO-CR-0229, Feb 2002.

64. Gassmann, O. and Meixner, H., eds, (2001) Biometric Authentication for Access Control, Sensors in Intelligent Buildings, Wiley-VCH Verlag GmbH.

65. Gassmann, O. and Meixner, H., eds, (2001) Smart Cameras for Intelligent Buildings, Sensors in Intelligent Environment, Wiley-VCH Verlag GmbH.

66. GEZ Microsystems, company information, last accessed October 2002, <http://www.gezmicro.com/>.

67. George, M.H., King, R.A. (1995), A robust speaker verification biometric Security Technology, Proc. IEEE 29th Annual 1995 Int. Carnahan Conf. on , 41-46.

68. Gross, R. Yan, J. and Waibel, A. (2000) Face Recognition in a Meeting Room, 4th IEEE Int. Conf. on Automatic Face and Gesture Recognition, Grenoble, France.

69. Gross, R. Yan, J. and Waibel, A. (2000) Growing Gaussian Mixture Models for Pose Invariant Face Recognition, Int. Conf. on Pattern Recognition ICPR 2000, Barcelona, Spain, 5088.

70. Gross, R., Matthews, I. and Baker, S. (2002) Appearance-Based Face Recognition and Light-Fields, Tech. Report CMU-RI-TR-02-20, Robotics Institute, Carnegie Mellon University.

71. Gross, R., Matthews, I. and Baker, S. (2002) Fisher Light-Fields for Face Recognition Across Pose and Illumination, Proc. German Symposium on Pattern Recognition (DAGM), 481-489.

72. Gross, R., Shi, J. and Cohn, J. (2001) Quo vadis Face Recognition?, 3rd Workshop on Empirical Evaluation Methods in Computer Vision.

73. Han, C, and Tsai, C. (2001) A multi-resolutional face verification system via filter-based integration, IEEE Annual Int. Carnahan Conf. on Security Technology, 278-281.

74. Guillevic, D., Suen, C.Y. (1995) Cursive script recognition applied to the processing of bank cheques, Document Analysis and Recognition, Proc. of the Third Int. Conf. , Vol 1 , 11-14.

75. Hamouni, S. (2002) Swedish school learns the value of biometrics, Conf. Proc. Biometrics 2002, London, UK.

76. Hashimoto, H. and Fukushima, K. (1999) Recognition and Segmentation of Components of a Face with Selective Attention, IEICE Trans. Systems and Computers in Japan, 30 (9) 2194-2202.

77. Heisele, B., Poggio, T. and Pontil, M. (2000) Face Detection in Still Gray Images, AI Memo 1687, Massachusetts Institute of Technology.

78. Hindus, L. (2000) A Finger, a Hand, an Eye and a Face: Biometric Imaging for Access Control, Advanced Imaging, 14-16.

79. Hjelmas, E. (2001) Face Detection: A Survey, Computer Vision and Image Understanding, 83 (3) 236–274.

80. Hong, L. and Jain, A. (1998) Integrating Faces and Fingerprints for Personal Identification, IEEE Trans. on PAMI, 20 (12) 1295-1307.

81. Hong, L., Wan, Y. and Jain, A. (1998) Fingerprint Image Enhancement: Algorithm and Performance Evaluation, IEEE Trans. on Pattern Analysis and Machine Intelligence, 20 (8) 779-789.

82. Hosticka, B. (2001) Smart Cameras for Intelligent Buildings, Sensors in Intelligent Buildings, Sensor Applications, Wiley-VCH Verlag GmbH, Vol 2.

83. Huang, R. (1998) Detection Strategies for Face Recognition using Learning and Evolution, PhD Dissertation, <http://cs.gmu.edu/~rhuang/dissertation.html>.

84. Hurley, D., Nixon, M. and Carter, J. (2000) A new Force Field Transform for Ear and Face Recognition, IEEE Int. Conf. on Image Processing ICIP2000, 25-28.

85. Infineon Technologies AG, company information, last accessed October 2002, <http://www.infineon.com>.

86. Information on Optasia, last accessed October 2002, <http://www.image-metrics.com>.

87. Jain, A. and Pankanti, S. (2000) Fingerprint Classification and Recognition, The Image and Video Processing Handbook, Bovik, A. Ed Academic Press April 2000. last accessed October 2002, <http:/biometrics.cse.msu.edu/publications.html>.

88. Jain, A., Griess, F. and Connell, S. (2002) On-Line Signature Verification, Pattern Recognition, 35 (12) 2963–2972.

89. Jain, A., Prabhabar, S. and Ross, A. (1999) Fingerprint matching: Data Acquisition and Performance Evaluation, TR MSU–CPS-99-14.

90. Johnson, R. (1997) Face Recognition Provides Security Alternative, Electronic Engineering Times, 07/07/97 Issue 961, 36.

91. Kamran, E. and Chellappa, R. (1996) Face recognition using discriminant eigenvectors, IEEE Int. Conf. on Acoustics, Speech and Signal Processing, 2148-2151.

92. Kozlay, D. (2002) The Arrival of the Fingerprint Smartcard, Biometrics Consortium Conference, NISTIR 6755.

93. Kroeker, K., Graphics and Security: Exploring Visual Biometrics, (2002), IEEE Computer Graphics and Applications, 22 (4) 16-21.

94. Kuprtstein, M. (1996) Face Recognition: the oldest way to verify ID is now the newest, in Defense and Security Electronics 28-31.

95. Lanitis, A. (2002) Toward Automatic Simulation of Aging Effects on Face Images, IEEE Trans. on Pattern Analysis and Machine Intelligence, 24 (4) 442-455.

96. Lauria, S. and Mitchell, R. (1999) Weightless Neural Nets for Face Recognition: A Comparison, Proc WIRN99, Vietri sul Mare (SA), Italy, 539-546.

97. Lawlor, M. (1997) Thermal Pattern Recognition System Faces Security Challenges Head On, Signal, 64-66.

98. Lee, K., Ho, J. and Kriegman, D. (2001) Nine Points of Light: Acquiring Subspaces for Face Recognition under Variable Lighting, IEEE Conf. Computer Vision and Pattern Recognition.

99. Leigh, S., Phillips, P., Grother, P., Heckert, A., Rukhiny, A., Newtonz, E., Moody, M., Kniskern, K. and Heath, S. (2002) Transformation, Ranking, and Clustering for Face Recognition Algorithm Comparison, 3rd Workshop on Automatic Identification Advanced Technologies (AutoID 02/IEEE), Tarrytown, NY.

100. Levin, G. (2002) Real World, Most Demanding Biometric System Usage, Biometric Consortium Conference, NISTIR 6755.

101. Lin, S., Kung, S. and Lin, L. (1997) Face Recognition/Detection by Probabilistic Decision-Based Neural Network, IEEE Trans. on Neural Networs, 8 (1) 114-132.

102. Lincoln, M. and Clark, A. (2000) Towards Pose-Independent Face Recognition, IEE Colloquium on Visual Biometrics, 5/1-5/5.

103. Lotlikar, R. and Kothari, R. (1998) Face recognition using curvilinear component analysis, IEEE World Congress on Computational Intelligence 3, 1778-1783.

104. Love, R. (2001) fMRI used to study race effect on face recognition, THE LANCET Vol 358.

105. Maio, D., Maltoni, R., Cappelli, J., Wayman, J. and Jain, A. (2002) FVC2002: Fingerprint Verification Competition, IEEE Trans. on PAMI, 24 (3) 402-411.

106. Mansfield, T., Kelly, G. Chandler, D. and Kane, J. (2001) Biometric Product Testing Final Report, Issue 1, National Physical Lab UK, 22.

107. Martinez, A. and Kak, A. (2001) PCA versus LDA, IEEE Pattern Analysis and Machine Intelligence, 23 (2) 228-233.

108. Mockensturm, L. (2002) Testing technology: From the lab to the field with facial recognition, Correction Today, June 2002.

109. Moon, H. and Phillips, P. (1998) Analysis of PCA-based Face Recognition Algorithms, Empirical Evaluation Techniques in Computer Vision, IEEE Computer Society Press, Los Alamitos CA, 57-71.

110. Nakamura, K. and Yoshikawa, T. (2001) Evaluation of Recognition Ability and Inside Parameters for a Rotation Spreading Associative Neural Network, Electronics and Communications in Japan (Part III: Fundamental Electronic Science) 84 (10) 1-14.

111. Navratil, J. Kleindienst, J. and Maes, S. (2000) An instantiable speech biometrics module with natural language interface: implementation in the telephony environment, IEEE Int. Conf. on Acoustics, Speech and Signal Processing, 2 (11) 1097-1100.

112. National Center for State Courts (NCSC), Williamsburg, Virginia, USA (URL: http://www.ncsconline.org/).

113. Neurodynamics Ltd, Cambridge, UK, company information, last accessed October 2002, <http://www.neurodynamics.com>.

114. Nixon, M. (1996) Dataveillance, 21+C, 30-6.

115. O'Hanlon, M. et al. (2002) Protecting the American Homeland, A Preliminary Analysis, Library of Congress Cataloging-in-Publication. ISBN 0-8157-0651-0.

116. Okada, K. and von der Malsburg, C. (2002) Pose-Invariant Face Recognition with Parametric Linear Subspaces, 5th Int. Conf. on Automatic Face and Gesture Recognition, Washington D.C., 71.

117. Orwell, G (1949) Nineteen Eighty-Four, NAL, May 1976.

118. Pankanti, S., Prabhakar, S., and Jain, A. (2002) On the Individuality of Fingerprints, IEE Trans. on PAMI 24 (8) 1010-1025.

119. Park, S. Kim, E., Hwang, E., Lee, Y. and Kim, H. (2001) Face detection for security system on the Internet, IEEE Int. Conf. on Consumer Electronics 2001, 276-277.

120. Pearce, R. (2001) Access Control and Biometrics, Security Electronics, August 2001, 36-40.

121. Pearce, R. (2001) Access Control: Implementing a Biometric System, Security Electronics Sep 2001, 18-20.

122. Penev P. and Atick J. (1996) Local Feature Analysis: A General Statistical Theory for Object Representation, last accessed October 2002, <http://citeseer.nj.nec.com/cache/papers/cs/403/ftp:zSzzSzvenezia.rockefeller.eduzSzgroupzSzpaperszSzfullzSzLFAzSzPenevPS.LFA.300.pdf/penev96local.pdf>

123. Petrou, M. and Bosdogianni, P. (1999), Image Processing: The Fundamentals, John Wiley & Sons Ltd Print ISBN 0-471-99883-4 Electronic ISBN 0-470-84190-7.

124. Philips, P., Martin, A., Wilson, C. and Przybocki, M. (2000) An Introduction to Evaluating Biometric Systems, Computer, 33 (2) 56-63.

125. Phillips, P. (2000) The FERET Evaluation Methodology for Face Recognition Algorithms, IEEE Trans. on Pattern Analysis and Machine Intelligence 22 (10) 1090-1104.

126. Phillips, P., Rauss, P. and Der, S. (1996) FERET (Face Recognition Technology) Recognition Algorithm Development and Test Results, Army Research Laboratory Adelphi, MD 20783-1197 ARL-TR-995.

127. Pike, G., Kemp, R. and Brace, N. (2000) The Psychology of Human Face Recognition, IEE Electronics and Communications: Visual Biometrics, 11/1-11/6.

128. Podilchuk, C. and Zhang, X. (1996) Face recognition using DCT-based feature vectors, IEEE Int. Conf. on Acoustics, Speech and Signal Processing, vol 4, 2144-2147.

129. Poulton, G. (2000) Facial Recognition: Practical Application of New Generation Biometrics, 6th Annual South Pacific Security and Access Control Conference (Access-2000), Brisbane, Australia.

130. Poulton, G. (2000) Facial Recognition:Practical Application of New Generation Biometrics, 6th Annual South Pacific Security and Access Control Conference, Brisbane, Australia.

131. Poulton, G. (2001) Face Recognition in Open Environments: Developments in CSIRO, Int. Symposium on Intelligent Multimedia, Video & Speech Processing, 494-497.

132. PriceWaterHouse Coopers, Australian Customs Service Biometric Technology Survey, client report, 109 pages.

133. Prokoski, F. (2000) History, current status, and future of infrared identification, IEEE Workshop on Comp. Vision, Beyond the Visible Spectrum: Methods and Applications (Cat. No.PR00640), Los Alamitos, CA, USA, 5-14.

134. Prototype, Fit to Print (2002), MIT Enterprise, technology Review, information last accessed October 2002, <http://techreview.com/articles/prototype50102.asp>.

135. Retina Scan Strengths and Weaknesses, last accessed October 2002, <http://retina-scan.com/retina-scan_strengths_and_weaknesses.htm>

136. Retina-Scan Technology, last accessed October 2002, <http://retina-scan.com/retina-scan_technology.htm>.

137. Rosen, L. and Friedman, W. Cryptoanalysis of German Army & German Air Force ENIGMA Traffic, SSA (report on) "E" Operations of the GCCS At Bletchley Park, 1945, 59. (NARA Record Group 457; File #3620.)

138. Security at your Fingertips (author unknown), No. 91 / February 2002 (magazine), Published by SAP AG Global Customer Affairs, Neurottstrasse 16, 69190 Walldorf, Germany.

139. Seitz, P. and Bichsel, M. (1991) 'The digital doorkeeper'–Automatic face recognition with the computer, 25th Carnahan Conf. on Security Technology, 77-83.

140. Shakhnarovich, G., Fisher. J and Darrell, T. (2002) Face recognition from long-term observations, European Conf. on Computer Vision, 851-868.

141. Shakhnarovich, G., Lee, L. and Darrell, T. (2001) Integrated Face and Gait Recognition From Multiple Views, IEEE Conf. Computer Vision and Pattern Recognition, 439-446.

142. Sherlock, B. and Monro, D. (1997) Balanced Uncertainty Wavelets for Fingerprint Compression, IEE Colloquium on Image Processing for Security Applications (IPSA'97), London, England, 5/1-6.

143. Smith, T. (2000) Smart Card Industry Review 2000, © 2002 Smart Card News Ltd, PO Box 1383, Rottingdean, Brighton, East Sussex, BN2 8WX United Kingdom, http://www.smartcard.co.uk/resources/articles/indreview-00.html

144. Silicon Valley Blue Ribbon Task Force on Aviation security and Technology (2002) Convened: M. Honda and R. Gonzales. Jun 2002.

145. Sim, T. and Kanade, T. (2001) Combining Models and Exemplars for Face Recognition: An Illuminating Example, Workshop on Models versus Exemplars in Computer Vision, CVPR.

146. Sim, T., Baker, S. and Bsat, M. (2002) The CMU Pose, Illumination, and Expression (PIE) Database, Int. Conf. on Automatic Face and Gesture Recognition, 53.

147. Sim, T., Sukthankar, R., Mullin, M. and Baluja, S. (2000) Memory-based Face Recognition for Visitor Identification, 4th Int. Conf. on Face and Gesture Recognition, Grenoble, France, 214-220.

148. Singletary, B. and Starner, T. (2001) Symbiotic Interfaces For Wearable Face Recognition, College Of Computing, Georgia Inst. of Tech, Atlanta, GA 30332.

149. Srihari, S. and Srihari, R. (1995) Written Language Input, in Survey of the State of the Art in Human Language Technology, Cole, R., Mariani, J., Uszkoreit, H., Zaenen, A. and Zue, V., Eds, National Science Foundation Directorate XIII-E of the Commission of the European Communities, 77.

150. Staedter, T. (2001) Face recognition: A camera and algorithm know it's you, Technology Review November 2001.

151. Stiefelhagen, R., Yang, J. and Waibel, A. (2001) Estimating Focus of Attention Based on Gaze and Sound, Workshop on Perceptive User Interfaces.

152. Sutherland, G., Ramsay, C., Renshaw, D. and Denyer, P. (1992) A comparison of vector quantisation codebook generation algorithms applied to automatic face recognition, BMVC'92, Leeds, 508-517.

153. Swan, P. (2002) DoD BMO Launches a New Website, last accessed October 2002, <http://www.c3i.osd.mil/biometrics/>.

154. Syed, A., Rizvi , P. Phillips, P. and Moon, H. (1998) The FERET Verification Testing Protocol for Face Recognition Algorithms, Int. Conf. on Face and Gesture Recognition, 48-53.

155. Symosek, P. (2000) The imaging issue in an automatic face/disguise detection system, IEEE Workshop on Comp. Vision Beyond the Visible Spectrum: Methods and Applications (Cat. No.PR00640) 15-24.

156. TEKEY Research Group, last accessed October 2002, <http://www.tekey.com/technology/disadvantage.html>.

157. Temdee, P., Khawparisuth, D. and Chamnongthai, K. (1999) Face Recognition by using Fractal Encoding and Back Propagation Neural Network, International Symposium on Signal Processing and its Applications, 159-161.

158. The Encyclopedia of Computer Security, (2000) http://www.itsecurity.com/bs.htm, TECS, 60 Churchfields Drive, Bovey Tracey, Devon, TQ13 9QU, UK, Townsend & Taphouse.

159. Titsworth, T., (2002) More than face value: airports and multimedia security, Multimedia, IEEE , 9 (2) 11-13.

160. The Functions of Biometric Identification Devices, National Biometrics Test Center, San Jose State University(information) last accessed October 2002, <http://www.engr.sjsu.edu/biometrics/publications_tech.html>.

161. Ultrascan, company information, last accessed October 2002, <http://www.ultrascan.com>.

162. Uszkoreit, H. (1995) Mathematical Methods, Survey of the State of the Art in Human Language Technology, Cole, R., Mariani, J., Uszkoreit, H., Zaenen, A., and Zue, V. () Eds, National Sciénce Foundation Directorate XIII-E of the Commission of the European Communities, 337.

163. Weber, R. (2000) Motorola's Experience with Biometrics: Unlocking Opportunities for Imaging, in Advanced Imaging, 15 (10), 22-24, 52.

164. Willaims, G. (1996) Iris recognition technology, 30th Int. Carnahan Conf. on Security Technology, 46-59.

165. Williams, G. (1997) Iris recognition technology, IEEE AES Systems Magazine, 23-29.

166. Wiskott, L. (1999) The Role of Topographical Constraints in Face Recognition, Pattern Recognition Letters 20 (1) 89-96.

167. Wiskott, L., Fellous, J., Kruger, N. and von der Malsburg, C. (1999) Face Recognition by Elastic Bunch Graph Matching, Intelligent Biometric Techniques in Fingerprint and Face Recognition Springer-Verlag, ISBN 0-8493-2055-0.

168. Woodward, J., Biometrics: facing up to terrorism. 2001, RAND Arroyo Center.

169. Woodward, J., Webb, K., Newton, E., Bradley, M. and Rubenson, D. (2001) Army Biometric Applications: Identifying and Addressing Sociocultural Concerns, Rand Arroyo publication ISBN O-8330-2985-1.

170. Xi, D., Podolak, I. and Lee, S. (2002) Facial Component Extraction and Face Recognition with Support Vector Machines, Fifth IEEE Int. Conf. on Automatic Face and Gesture Recognition Washington D.C., 83-88.

171. Yang, J., Yu, H. and Kunz, W. (2000) An Efficient LDA Algorithm for Face Recognition, The Sixth International Conference on Control, Automation, Robotics and Vision.

172. Yu, H. and Yang, J. (2000) A direct LDA algorithm for high-dimensional data with application to face recognition, in Pattern Recognition 34, 2067-2070.

173. Zhang, M. and Fulcher, J. (1996) Face perspective understanding using artificial neural network group-based tree, IEEE ICIP(C), 475-478.

174. Zhang, M. and Fulcher, J. (1996) Face Recognition Using Artificial Neural Network Group-Based Adaptive Tolerance (GAT) Trees, IEEE Trans. on Neural Networks, 7 (3), 555-567.

175. Zhao, W., Chellappa, R., Rosenfeld, A. and Phillips, P. (2000) Face Recognition: A Literature Survey, lUMD Technical Report, CAR-TR-948.

176. Zue, V. and Cole, R. (1995) Spoken Language Input, Survey of the State of the Art in Human Language Technology, Cole, R., Mariani, J., Uszkoreit, H., Zaenen, A. and Zue, V. Eds, National Science Foundation Directorate XIII-E of the Commission of the European Communities.

DISTRIBUTION LIST

Biometrics Technology Review

T Blackburn, M Butavicius, I Graves, D Hemming, V Ivancevic, R Johnson, A Kaine, B McLindin, K Meaney, B Smith and J Sunde,

AUSTRALIA

DEFENCE ORGANISATION

Task Sponsor **Chief, Land Operations Division**

S&T Program

Chief Defence Scientist
FAS Science Policy
AS Science Corporate Management
Director General Science Policy Development
} shared copy

Counsellor Defence Science, London (Doc Data Sheet)
Counsellor Defence Science, Washington (Doc Data Sheet)
Scientific Adviser to MRDC Thailand (Doc Data Sheet)
Scientific Adviser Joint
Navy Scientific Adviser (Doc Data Sheet and distribution list only)
Scientific Adviser - Army (Doc Data Sheet and distribution list only)
Air Force Scientific Adviser
Director Trials

Systems Sciences Laboratory

Research Leader Human Systems Integration (Doc Data Sheet and Distribution Sheet Only)
Author(s):
J Sunde
M Butavicius
I Graves
D Hemming
V Ivancevic
A Kaine
B McLindin
K Meaney
B Smith
T Blackburn (c/- J Sunde)
R Johnson (c/- J Sunde)

DSTO Library and Archives
Library Edinburgh 2 copies
Australian Archives

Capability Systems Division
Director General Maritime Development (Doc Data Sheet only)
Director General Land Development
Director General Aerospace Development (Doc Data Sheet only)
Director General Information Capability Development (Doc Data Sheet only)

Office of the Chief Information Officer

Chief Information Officer (Doc Data Sheet only) (
Deputy CIO (Doc Data Sheet only)
Director General Information Policy and Plans (Doc Data Sheet only)
AS Information Structures and Futures (Doc Data Sheet only)
AS Information Architecture and Management (Doc Data Sheet only)
Director General Australian Defence Information Office (Doc Data Sheet only)
Director General Australian Defence Simulation Office (Doc Data Sheet only)

Strategy Group

Director General Military Strategy (Doc Data Sheet only)
Director General Preparedness (Doc Data Sheet only)

HQAST

SO (ASJIC) (Doc Data Sheet only)

Navy

SO (SCIENCE), COMAUSNAVSURFGRP, NSW (Doc Data Sheet and distribution list only)
Director General Navy Capability, Performance and Plans, Navy Headquarters (Doc Data Sheet Only)
Director General Navy Strategic Policy and Futures, Navy Headquarters (Doc Data Sheet Only)

Army

ABCA National Standardisation Officer, Land Warfare Development Sector, Puckapunyal (4 copies)
SO (Science), LHQ, Victoria Barracks, Paddington NSW 2021 (Doc data sheet and Executive Summary only)
SO (Science), Deployable Joint Force Headquarters (DJFHQ) (L), Enoggera QLD (Doc Data Sheet only)

Air Force

Director General Policy and Plans, Air Force Headquarters (Doc Data Sheet only)
Director General Technical Air Worthiness, RAAF Williams (Doc Data Sheet only)
Chief of Staff – Headquarters Air Command, RAAF Glenbrook (Doc Data Sheet only)
Commander Aircraft Research and Development Unit, RAAF Edinburgh (Doc Data Sheet only)
Commander Air Combat Group, RAAF Williamtown (Doc Data Sheet only)
Staff Officer (Science), RAAF Amberley (Doc Data Sheet only)
Staff Officer (Science), RAAF Williamtown (Doc Data Sheet only)
Commander Air Lift Group, RAAF Richmond (Doc Data Sheet only)
Commander Maritime Patrol Group, RAAF Edinburgh (Doc Data Sheet only)
Commander Surveillance Control Group, RAAF Williamtown (Doc Data Sheet only)
Commander Combat Support Group, RAAF Amberley (Doc Data Sheet only)
Commander Training, RAAF Williams (Doc Data Sheet only)

Intelligence Program

DGSTA Defence Intelligence Organisation
Manager, Information Centre, Defence Intelligence Organisation
Assistant Secretary Corporate, Defence Imagery and Geospatial Organisation (Doc Data Sheet only)

Defence Materiel Organisation

Head Airborne Surveillance and Control (Doc Data Sheet only)
Head Aerospace Systems Division (Doc Data Sheet only)
Head Electronic Systems Division (Doc Data Sheet only)
Head Maritime Systems Division (Doc Data Sheet only)
Head Land Systems Division (Doc Data Sheet only) (

Defence Libraries

Library Manager, DLS-Canberra (Doc Data Sheet Only)
Library Manager, DLS - Sydney West (Doc Data Sheet Only)

Australian Customs Service

c/- Ranald Kennard, Manager, Traveler Strategies, Customs House, 5 Constitution Ave, Canberra ACT 2601 (3 copies)

UNIVERSITIES AND COLLEGES

Australian Defence Force Academy
Library
Head of Aerospace and Mechanical Engineering
Hargrave Library, Monash University (Doc Data Sheet only)
Librarian, Flinders University

OTHER ORGANISATIONS

National Library of Australia
NASA (Canberra)
State Library of South Australia

OUTSIDE AUSTRALIA

INTERNATIONAL DEFENCE INFORMATION CENTRES

US Defense Technical Information Center, 2 copies
UK Defence Research Information Centre, 2 copies
Canada Defence Scientific Information Service, 1 copy
NZ Defence Information Centre, 1 copy

ABSTRACTING AND INFORMATION ORGANISATIONS

Library, Chemical Abstracts Reference Service
Engineering Societies Library, US
Materials Information, Cambridge Scientific Abstracts, US
Documents Librarian, The Center for Research Libraries, US

INFORMATION EXCHANGE AGREEMENT PARTNERS

Acquisitions Unit, Science Reference and Information Service, UK
Library - Exchange Desk, National Institute of Standards and Technology, US

SPARES (5 copies)

Total number of copies: **52**

DEFENCE SCIENCE AND TECHNOLOGY ORGANISATION
DOCUMENT CONTROL DATA

1. PRIVACY MARKING/CAVEAT (OF DOCUMENT)

2. TITLE

Biometrics Technology Review 2002

3. SECURITY CLASSIFICATION (FOR UNCLASSIFIED REPORTS THAT ARE LIMITED RELEASE USE (L) NEXT TO DOCUMENT CLASSIFICATION)

Document	(U)
Title	(U)
Abstract	(U)

4. AUTHOR(S)

T Blackburn, M Butavicius, I Graves, D Hemming, V Ivancevic, R Johnson, A Kaine, B McLindin, K Meaney, B Smith and J Sunde

5. CORPORATE AUTHOR

Systems Sciences Laboratory
PO Box 1500
Edinburgh South Australia 5111 Australia

6a. DSTO NUMBER	6b. AR NUMBER	6c. TYPE OF REPORT	7. DOCUMENT DATE
DSTO-GD-0359	AR 012-602	General Document	March 2003

8. FILE NUMBER	9. TASK NUMBER	10. TASK SPONSOR	11. NO. OF PAGES	12. NO. OF REFERENCES
E9505-25-22	STR 01/358	Chief LOD	42	176

13. URL on the World Wide Web

http://www.dsto.defence.gov.au/corporate/reports/DSTO-GD-0359.pdf

14. RELEASE AUTHORITY

Chief, Land Operations Division

15. SECONDARY RELEASE STATEMENT OF THIS DOCUMENT

Approved for public release

OVERSEAS ENQUIRIES OUTSIDE STATED LIMITATIONS SHOULD BE REFERRED THROUGH DOCUMENT EXCHANGE, PO BOX 1500, EDINBURGH, SA 5111

16. DELIBERATE ANNOUNCEMENT

No Limitations

17. CITATION IN OTHER DOCUMENTS Yes

18. DEFTEST DESCRIPTORS

Identification systems
Security systems
Face recognition
Speech recognition

19. ABSTRACT

The September 11 2001 terrorist attacks in the USA have motivated renewed global efforts to secure national borders and accordingly Australian authorities have demonstrated an interest in mechanisms that support these endeavours. This report examines the current state of biometric technologies, characterises the main categories and focuses on face recognition, which is the least intrusive but most effective means of applying filters at access points to the country. It also reviews some of the ramifications of large scale surveillance measures when applied to populations.