Edith Cowan University
Research Online

ECU Publications Pre. 2011

1997

Review of personal identification systems

J. M. Cross
Edith Cowan University

Follow this and additional works at: https://ro.ecu.edu.au/ecuworks

 Part of the Information Security Commons

Cross, J.M. (1997). *Review of personal identification systems*. Perth, Western Australia: Edith Cowan University.
This Report is posted at Research Online.
https://ro.ecu.edu.au/ecuworks/7280

Edith Cowan University

Copyright Warning

You may print or download ONE copy of this document for the purpose of your own research or study.

The University does not authorize you to copy, communicate or otherwise make available electronically to any other person any copyright material contained on this site.

You are reminded of the following:

- Copyright owners are entitled to take legal action against persons who infringe their copyright.

- A reproduction of material that is protected by copyright may be a copyright infringement. Where the reproduction of such material is done without attribution of authorship, with false attribution of authorship or the authorship is treated in a derogatory manner, this may be a breach of the author's moral rights contained in Part IX of the Copyright Act 1968 (Cth).

- Courts have the power to impose a wide range of civil and criminal sanctions for infringement of copyright, infringement of moral rights and other offences under the Copyright Act 1968 (Cth). Higher penalties may apply, and higher damages may be awarded, for offences and infringements involving the conversion of material into digital or electronic form.

FACULTY OF SCIENCE, TECHNOLOGY AND ENGINEERING
Australian Institute of Security and Applied Technology

RESEARCH REPORT

Review of Personal Identification Systems

J M Cross

April,1997
ISSN: 1324-6976
ISBN: 0-7298-0338-4

EDITH COWAN UNIVERSITY
PERTH WESTERN AUSTRALIA

EDITH COWAN UNIVERSITY
LIBRARY 00509/09/20

Edith Cowan University
Australian Institute of Security and Applied Technology

Review of Personal Identification Systems

J.M. CROSS

Edith Cowan University
Perth, Western Australia
J.Cross@cowan.edu.au

ABSTRACT

The growth of the use of biometric personal identification systems has been relatively steady over the last 20 years. The expected biometric revolution which was forecast since the mid 1970's has not yet occurred. The main factor for lower than expected growth has been the cost and user acceptance of the systems. During the last few years, however, a new generation of more reliable, less expensive and better designed biometric devices have come onto the market. This combined with the anticipated expansion of new reliable, user friendly inexpensive systems provides a signal that the revolution is about to begin. This paper provides a glimpse into the future for personal identification systems and focuses on research directions, emerging applications and significant issues of the future.

Review of Personal Identification Systems
J. M. Cross

Introduction

In order to restrict access of a person to buildings, facilities, computer systems, information, welfare payments or financial transfers it is necessary to be able to identify the person who is seeking access. Personal identification is a process that people use during every business and social encounter. However, with the complexities of modern society and the move to greater reliance on technology, we realise that the identification of an individual is no longer a simple task. Unfortunately technologies such as communication, computer and electronic systems are also being used increasingly for criminal activities. The security risk is further compounded with the increased value of assets, increased access flow and the use of automated systems in preference to manual systems. The only solution is to use these same technologies to provide for improved personal identification and therfore increase the level of security.

The traditional model of the identification process consists of three building blocks:

- something a person knows (codes)
- something a person possesses (cards)
- something about a person (characteristics).

Identification based on knowledge include for example personal identification numbers (PIN), passwords and encryption keys. Identification based on possession include for example the use of keys, ID badge, drivers license, magnetic stripe card, proximity card, wiegand card, smart card, optical storage card and the PCMCIA computer card. Identification based on characteristics are called biometrics and include physical or behavioral characteristics such as fingerprint or signature.

The three basic identification methods can be combined to give greater levels of protection as required. Allowing for these combinations there are seven conceptual alternatives or sections for protection. For example, access to a Automatic Teller Machine (ATM) requires the use of a swipe card and a PIN. This provides an additional level of protection if the card is lost or stolen.

The choice of the method for identification will depend on the level of security risk which in turn will depend on the value of the asset to be protected, the system characteristics including the vulnerability of the system to attack, types of threats, the user acceptance of the identification method and the cost of protection. As these features change with time the choice of an appropriate identification method will not be static. Movement within the dynamic model can occur due to automation or migration.

Automation occurs when an existing process is modernised to reduce costs, to improve quality or to handle greater volume. For example, picture ID badges, driver's licenses and even some credit cards are made using electronic video imaging instead

of still cameras. Not only does this speed up the process but the image can also be stored in the computer system for future reference and comparison. Migration occurs when the new approach to identification is in a different section of the model. This can occur to improve security level, to speed access flow, to reduce cost or add convenience.

Personal identification systems based on knowledge and/or possession offer limited security as they can be compromised. They are open to abuse because such systems identify a token or something known and not the actual person. In the case of a remotely accessed computer for instance, if its password is a dictionary word then security can be breached by trial and error; for example, a user can write a program that attempts to access the remote computer by exhaustively selecting words from an electronic dictionary. In the case of stolen or lost cash/credit cards, it is surprising "to learn that over a quarter of . . . cards which are recovered through the system have their activating PIN written on them" [14]. The obvious solution to improving security is to use biometric identification. This paper will focus on developments in this area and provide a glimpse into the future use of such systems.

Biometric Identification

Biometric systems are defined as *methods of verifying or recognising the identity of a living person based on physiological or behavioral characteristics.* The term biometric is used as the technology is based on *measurements* of *biological* traits of the subject.

Commercially available automatic systems have exploited such physiological characteristics as fingerprints, hand geometry, facial features and eye features and behavioral characteristics such as speech, signature dynamics and keyboard typing rhythms. These will be considered in detail later in this paper. Other possibilities for biometric access that may be commercialised in the future include personal odor and gait.

An *automatic* biometric system involves three major components:

- mechanism to scan and capture an image of a living persons characteristics
- compression, processing and comparison of image
- interface with application systems.

All biometric systems require each authorised user to be enrolled. This involves the user presenting the characterising trait to the system one or more times. A library template or signature is then formed from this sample. This template may be stored in a database or encoded on a card. Subsequently, when the user wishes to gain access, the characteristic trait must be presented to the system which then compares this against a single template for verification or a multitude of templates for recognition. In most access control situations we usually rely on biometrics for verification of an individual. The question being addressed is "Are you who you say you are?" instead of "Do I know who you are?".

The emphasis of biometric technology as opposed to forensic technology is on the identification of living persons. Good biometric systems should be able to differentiate living persons from substitutes such as latex fingers, digital audio tapes, plaster hand, prosthetic eye etc.

Both physiological and behavioral characteristics can be use in biometric systems. Physiological characteristics are relatively stable while behavioral characteristics because they involve a reflection of a persons psychological makeup are more variable. This means that behavioral systems require more often enrollment updates and are prone, in general to more errors. On the positive side behavioral systems tend to be more user friendly and in general, use less expensive sensor technology.

The performance and applicability of biometric systems depends upon many factors including:

(i) whether or not the client population is closed or open; e.g. a population of factory workers as opposed to the population of potential automatic teller machine users,
(ii) the false rejection rate(FRR) and false acceptance rates (FAR),
(iii) user reticence,
(iv) whether or not the technique is invasive,
(v) ease of use,
(vi) hygiene, and
(vii) cleanliness;

It is not surprising therefore that "a range of biometric systems is in development or in the market, because no one system meets all needs" [12].

The FRR and FAR which are also called Type I and Type II errors are important quantitative measures of the performance of the system and are usually expressed as percentages. The FRR is the rate of rejecting authorised users while the FAR is the rate of accepting impostors. Different applications will have different error specifications. For example, financial institutions seek systems with low FRR ,of say, less that 0.2% as they do not want to loose their clients to their competitors. On the other hand at strategic facilities of high value, such as a nuclear power plant, the FAR must be as low as possible even if say 5% of authorised users are rejected. Despite this variation the FRR and FAR rates for biometric systems are significantly lower that identification based on knowledge or possession.

The FRR and FAR are not independent but are inversely related. By setting the matching threshold within the biometric system to reduce the FRR it is likely to increase the FAR. A balanced system is one that has FRR and FAR at the same acceptable level. The best such system currently on the market is the hand geometry biometric which has a FRR-FAR crossover of less that 0.2%. Developers continue to work on techniques to reduce the FRR without any increase in the FAR. In addition, good training of the users of the system can also significantly reduce the rejection levels. This reinforces the need for the developers and owners of the systems to provide comprehensive support of their systems including training.

The growth of the use of biometric identification systems has been relatively steady over the last 20 years. The expected biometric revolution which was forecast since the mid 1970's has not yet occurred. Currently it is estimated that less than 20 000 facilities worldwide are using biometric identification systems. The main factor for lower than expected growth has been the cost and user acceptance of the systems that are available on the market. The average cost of a system 5 years ago was over US$6000. This has come down to US$2 000. There are however clear signals that this is about to change.

During the last few years a new generation of more reliable, less expensive and better designed biometric devices have come onto the market. In 1996 alone it is expected that at least 10 new fingerprint ,4 hand geometry and 2 voice recognition systems will be launched onto the market as well as new versions of existing products. Many of these systems will be sold for under US$500 with further reductions expected as production volume increases. With greater penetration into society and better system support they will be more readily accepted by society for a much wider range of applications. In the next section of this paper each of the biometric technologies will be considered including new research directions and applications.

Fingerprint Patterns

The use of a fingerprint has been the traditional biometric for identification of an individual. For centuries police have used fingerprints to identify criminals. For most of that time the prints have been laboriously matched by human experts. The fingerprint is unquestionably still the most reliable source of personal identification. It is estimated that the chance of two people, including twins, having the same print is less than one in a billion. The characteristics of a fingerprint can be identified by the shape of ridge or furrow lines and feature points called *minutiae.* Minutiae are identified as end points of a ridge (ridge endings) or branching of a ridge (bifurcation) as indicated in Figure 1.

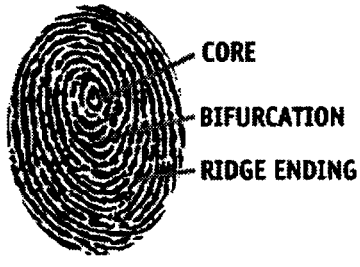

Figure 1. Minutiae

With the introduction of computers and electronic sensors came the ability to capture, process, store and match fingerprint patterns using sophisticated software. The most complex and expensive systems, with huge databases of more than a million stored images, are used by police agencies. The Federal Bureau of Investigation's Integrated Automated Fingerprint Identification System, for example, stores 40 terabytes of data.

The algorithms for the automated identification of criminals was developed by the FBI in the 1950's in conjunction with the National Bureau of standards , Cornell Aeronautical Laboratory, and Rockwell International Corp. A decade later several other companies entered the field basing their efforts on the early work of the FBI. The classical approach used involves pre-processing the digitally scanned image, edge detection, thresholding, binarisation, thinning, feature extraction and storage. The whole process can be very computationally expensive and hence requires more expensive hardware to meet the response time requirements.

Recently costs have begun to drop and the automated fingerprint identification systems are being considered for other than law enhancement. For example, the Los Angeles County uses such a system to ensure that welfare recipients apply for benefits only once.

The first commercial automated system had its origins in 1971 which was finally marketed in 1983 by Identrix Inc, Sunnyvale, California.

The Identrix system uses a compact terminal that incorporates light, lens, and charged-couple-device (CCD) image sensors to take high resolution picture of the fingerprint. To enroll, a user is assigned a personal identification number and then puts a single finger on a glass plate for scanning by the CCD image sensor. The 250 KB image is digitised and analysed. The result is a 1 KB mathematical characterisation of the fingerprint. The whole process takes about 30 seconds. Identity verification takes less than 1 second. The equipment usually gives the user three attempts for acceptance or final rejection. With the first attempt the rejection is over 3% in independent tests and false acceptance is less than 0.0001%. Each stand alone system can store up to 48 fingerprint templates with the price ranging from a two thousand to tens of thousands of dollars depending on the application and the number of terminals to be networked.

Currently the Identrix system (TouchSafe and TouchSafe II) is being used in over 40 countries [17]. Its applications include controlling access to physical space, computer networks, automated banking terminals, custom and immigration and prison control. As might be expected fingerprint verifiers are installed at military facilities such as the Pentagon and government laboratories. Banks, jails and commercial establishments are also early adopters. The largest worldwide application of fingerprint verification in the financial industry is being used for the distribution of 550 000 recipients in South Africa by the First National Bank of South Africa. The bank is using a cash Paymaster Services pension payment systems and employs over 1 000 ATM machines mounted in trucks. The pensions are distributed after the Identrix TouchSafe verification Terminal verifies the identity of the recipient. The system is reported to save the bank from $13 to $20 million Australian dollars per year. Another application is the bank card system in the Czech Republic, supplied by the Lasercard Systems Coporation. The identity of bank customers is verified using the Touchsafe Verification Terminals at the point of sale.

Quite a few newcomers have entered the field recently using a new generation of processing algorithms and feature extraction in order to reduce response-time and cost. At least 15 fingerprint identification products are now on the market. Systems are now available which can be integrated with smart cards for template storage that

the user can carry. The use of smart card technology for verification will reduce the need for large central databases and hence reduce costs.

One of the newcomers is an Australian based consortium of companies called Fingerprint Technologies. This consortium was established to meet the need for complete fingerprint recognition systems. The consortium includes Corban Australia Pty Ltd, Coretech and Base2. In 1995 the consortium released fully integrated systems based on fingerprint recognition aimed at specific applications. Two of their products are Fingerprint Sentry, a visitor identification and tracking application, and BioClock, a biometric time and attendance application. These systems include not only capture and matching of fingerprints but also provide for exporting, reporting and system and audit logging.

Several companies also claim to be developing or have obtained templates of under 100 bytes. For example, late last year Central Research Labs and TMS unveiled their fingerprint systems which have 60 and 26 byte templates respectively. Of the 17 known products that are under development it is expected that at least 10 will be released in 1996. There is considerable research being undertaken in universities and industry on the use of neural networks for matching, the use of fuzzy logic for feature extraction and the implementation of very large scale integrated chips [15].

Research is also being undertaken into alternative sensor technology to provide for improved image quality of the fingerprint. Studies of fingerprint technology have revealed that consistency and quality of data captured is a major issue with some 33% of records received at the UK National Identification Bureau being rejected for one reason or another.

The use of holograms and ultrasound have been proposed as a means of obtaining a better optical image than traditional scanners. Ultrasound has been explored as a means of obtaining good prints even when dirt is obscuring the print. Recently Ultra-Scan demonstrated an ultrasound fingerprint capture device which gives high quality images regardless of conditions. Advanced Precision Technology has developed a system using images stored holographically in a card.

Research is also currently underway on the use of a new tactile sensor. A prototype sensor which occupies an area of 12.8mm x 12. 88mm has been produced by Personal Biometric Encoders Limited which captures a frame of data comprising 16 348 pixels on contact with the fingertip. A thin layer of plastic covered with microscopic metal tiles conforms to the shape of the finger and activates a silicon based resistive matrix array of contact switches. A graphics image is obtained which gives an accurate facsimile of the fingerprint including sweat pores locations.

It has been found that the location of sweat pores (STARS) in relation to ridge endings (PLANETS) provides sufficient data for verification. To support the sensor the PCMCIA memory card (a PC card) is being considered in which the tactile sensor is embedded. The memory requirements for the fingerprint template is nominal enabling the PC card to include other functions and therefore serve as a universal access control device. As a secure verifier, the PC card can serve as an ID card, a driving license, a secure credit card, a medical records card and even an electronic passport.

The production of silicon based sensors has been the subject of detailed study. First indications are that the cost of a sensor embedded in a PCMCIA Memory Card should be between $5 and $10 in large volume production of 10 million units or more. At this level of cost the technology becomes an attractive option for general identification applications.

Another direction of research is the use of new optical computing techniques. One such system that is in its final Beta testing is the Canadian Zebra True Recognition developed by Mytec. Instead of a relying on digital technology the Zebra system will use the latest optical technology to capture and process the fingerprint at the speed of light and verification will take place in a fraction of a second. Not only will there be an increase in speed but reliability will be improved as the recognition will be based on the whole print rather than selected features. This has the potential to improve recognition when people get dirt, scratches, or cuts on their fingerprints. With the optical system such areas on the fingerprint will be ignored. Despite the 2 KB template configurations with optical card and smart cards will be available.

Another area of research has been the development of fingerprint systems, combined with a random number, as a key, for use in the encryption of data. This has wide ranging implications for the way business is conducted over networks, such as the secure transfer of information ,including data and financial transactions, over the internet. In addition, the fingerprint can be used to protect the privacy of an individual. With the development of smart cards and optical storage capabilities there will be a capacity for storage of large amounts of information on the card, So, in addition to the potential for fraud, if the card gets in the wrong hands it may lead to a breach of personal information. Fortunately, with the new technologies being developed a fingerprint can be stored in an encrypted form or "biocrypt" on the card. Each "biocrypt" is a unique, random - appearing pattern which is extremely difficult to be converted back to the original fingerprint. In this way the fingerprint can be used as a key which provides secure access to information stored on the card.

Hand Features

Hand Geometry is considered as the first automated biometric identification system on the market with over 20 years history of live applications. During this time over six hand scanning products have been developed but only one commercially viable product, the ID3D HandKey hand geometry system developed by Recognition Systems Inc., Campbell, California, dominates the market.

For the ID3D system the user punches in an identification code , then positions their hand on a plate between a set of guidance pins. Looking down upon the hand is a CCD digital camera, which with the help of side mirrors captures the side and top view of the hand simultaneously. The digitised image is analysed using a built in microprocessor to extract the identifying characteristics from the hand. The characteristics include measurements and comparison of finger and hand geometry. The resulting template is a 9 byte identity feature vector that is stored in the system during enrollment. Alternately the template is small enough to be stored on a magnetic swipe card. With this amount of data compression, the current 4.5kg unit,

with a single printed circuit board can store 20 000 identities. The enrollment of individuals involves taking three hand readings and averaging the resulting vectors. The ID3D is seen as the most balanced biometric device today which has scored FRR-FAR crossover of less than 0.2 % in independent tests. The minimum configuration of the system that can recognise 256 hands costs approximately $3000.

Hand Geometry is employed at over 6000 locations including access to operations at San Francisco International Airport, Lotus Development Corporation and to nuclear power plants in the United States. It is also being trialled at Kennedy and Newark International Airports for automated passport inspection and entry control of people who are registered as frequent flyers. Novel applications include its use in the Colombian House of Representatives and Senate to eliminate voting fraud and at a Los Angeles sperm bank. It is estimated that over 3000 units are being installed each year. This is expected to grow in the near future.

A major test of the system for large scale access control will occur this year at the Olympic games in Atlanta. Hand Geometry will be used to secure the athletes' village. Forty thousand volunteers will need to be enrolled along with all competing athletes, trainers and staff members. There will be 125 hand geometry verification devices installed to provide access to the village and other high security areas.

Other systems for hand recognition have been attempted but few have come to market until recently. Four systems that have entered the market recently are Fingerscan, Digi-2 by Biomed, Hand Punch and HandMark XO by Pideac. Each of these systems use different characteristics of the hand for verification. The Fingerscan system, developed in Australia, is an opto-electronic finger scanning device that records "three-dimensional data from the finger such as skin undulations, ridges and valleys, reflections and other living characteristics" [16]. The Digi-2 system uses 3 dimensional measurements of two fingers only and sells for less than $700. While the template size is approximately 20 bytes the system has a FAR-FRR balance close to 0.1%. The Handpuch system is a biometric time clock which is designed for the time and attendance market. It uses the size and shape of the hand and is being used in hospitals, law offices, nursing homes, casinos and various manufacturing companies.

The latest product to be released commercially is the HandMark XO system by Pideac. This system records the peaks and valleys of the users knuckle profile. The knuckle profile is obtained by the user gripping a bicycle-like hand grip and rotating it 90 degrees until it encounters a stop at the horizontal. One novel application envisaged for the system is the installation on the dashboard of the car to prevent car jacking. The system is available in several versions for verification including a smart card, magnetic stripe card, a wiegand card, a proximity card, a touch screen or keypad and a no card, no keypad version for recognition of the user from the database. The system is available for between $1300 and $3000 depending on options and quantity.

There are quite a few hand recognition systems under development. New characteristics of the hand are being examined for potential for identification. Several systems, such as Bio Density, Fastpass by Biometrics Inc and PG-2001 by Talos Technology are capturing small portions of the palm and/or fingers. Features such as the creases on the palm or fingers will be used for verification. The aim of these

systems is to reduce the size of the sensor and hence reduce cost while maintaining FAR-FRR balances at 0.1%.

Another approach that is undergoing considerable research and development is the use of vein patterns on the back of the hand for identification. This system, first reported by MacGregor and Welford (1991), involves verifying user identity on the basis of the pattern of subcutaneous veins on the back of the hand [8,9].

The pattern of veins on the back of the hand is particularly interesting because, although the veins are constrained to run between the bones of the knuckles to connect to the fingers, and are constrained where they run over the wrist bones, in between they seem to conform to no particular pattern. Nevertheless the vein pattern seems to be stable over a period of years [5].

This technique shows promise as a passive, non-invasive means of personal identification. It must be stressed though that the viability of this concept has yet to be established. Hypothesis testing (statistical inference) is needed to determine the validity of the premise that a person's hand vein pattern is unique. To this end it is necessary to build a research biometric system capable of acquiring, automatically processing, and matching vein pattern images; and for which the false acceptance rate (FAR) and false rejection rate can be established. Cambridge Consultants Ltd., in collaboration with the British Technology Group (BTG), have been researching the hand vein pattern concept (which they have called *Veincheck*) with the aim of developing a commercial system.
Their system is planned to be released onto the market later this year. After much experimentation they have opted to develop the capture system into an intelligent door handle. The vein pattern from the back of the hand is captured in the near infrared range. A light source is used which is reflected from the hand back to the CCD camera. A template of approximately 400 bytes which mathematically describes the vein pattern will be used as the template.

The Australian Institute of Security and Applied Technology (AISAT), at Edith Cowan University, has also been independently examining, since 1993, the use of vein patterns on the back of the hand as a suitable biometric for identification. The author of this paper has been a member of the research team. In 1994 the team outlined a low cost infrared (IR) imaging system and semi-automatic segmentation algorithm for the extraction of a vein signature from a digital infrared image of the back of a person's hand [2]. During 1995 the AISAT research team refined the imaging system and segmentation algorithms (now completely automatic) and additionally implemented and evaluated a custom matching algorithm [10]. Details of the image acquisition system, the image processing algorithms and statistical tests are outlined in a number of papers which have been presented in reports and in conference publications both in Australia and the United Kingdom [3, 11]. The prototype system we developed uses a cold IR light source and standard CCD security camera for capture. An example of a hand the vein pattern is shown in figure 2. The tests undertaken confirmed that the system performs extremely well using low cost hardware which is already available off the shelf.

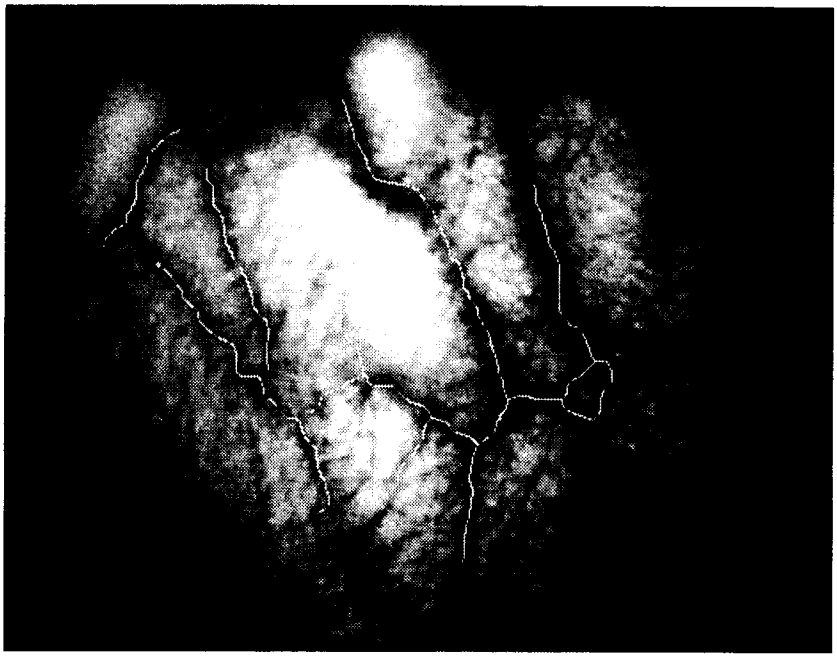

Figure 2. Digital image of back of hand and the vein template

A further area of hand biometric research, that has also been undertaken at AISAT, is the use of true three dimensional imaging. This has proved to be a very difficult area due to calibration problems associated with the use of multiple cameras. The results of applying a three dimensional range imaging system, based on coded structured light has been presented by one of the AISAT researchers [18].

Facial Features

The use of facial features for personal identification is the primary method used by humans. Much research has been undertaken in recent times to develop an automated facial verification or recognition system using approaches ranging from pattern recognition using neural networks to infrared scans of "hot spots" on the face. Despite the best efforts of government and industry research laboratories only a few systems have made it to the market. Despite the challenges involved in facial recognition there is considerable interest in the approach particularly from law enforcers.

Using the whole face for automatic identification is a complex task because the appearance is constantly changing. Variations in facial expression, hair style and facial hair, head position, camera scale and lighting create images that usually differ from those captured earlier. Artificial neural networks which enable the computer to learn and adapt and be taught to recognise patterns were developed in the 1950's and 1960's and have been applied for use in recognition of facial features. The NeuroMetric Vision System introduced in 1992 and, more recently, the Intelligent Vision System and the True Face System by Miros are based on the use of neural networks for recognition. A scan is first obtained of the face. Processing involves geometric scaling and rotation, compensation for lighting differences and

mathematical transformations to reduce the face to a set of feature vectors. The feature vector is the input to the neural network trained to respond to matching it to one of the trained images.

Using standard video and computer hardware, the system compares a live face image with the previously recorded face image. The current systems need to accommodate wide variability of how a person's face can look at different times yet at the same time detect impostors. For the matching process the TrueFace system, for example, computes the level of match and returns a number in the range of 0 -10 as a level of confidence within 1 second. This level is compared against a preset threshold. The threshold can be set to provide an acceptable level of false rejects at the expense of false acceptances. The FRR - FAR crossover point for the TrueFace system has been shown to be 1.75%.

For the enrollment process a person's picture and ID information can be stored onto a storage medium on a plastic card or on a computer chip in a smart card or in a database. To reduce storage requirements, the person's face is automatically located, clipped out and compressed. For the systems such as TrueFace the enrollment process, not including time for entering ID information, can be completed within 1 second. The size of the template for the facial image features is currently approximately 2 Kb which is comparable to the fingerprint template.

A specialised application of the facial recognition system has just been released by Siemens Nixdorf. They have developed an automatic teller machine based on neural networks that identifies users by their faces. A ProCash ATM has been introduced that authenticates users by their physical features and checks whether they are authorised to withdraw cash. The system replaces conventional entry of a PIN and is suitable for installation in equipment of the CSC/430 and CSC/450 systems families.

When the user inserts his smart card, a camera integrated in the ATM automatically takes a photograph of the user's face and compares the facial features with the reference image stored on the card. The read device automatically deletes the verification data when the cardholder withdraws cash. It stores the image of the user only if illegal access is attempted. This enables the transaction to be reconstructed and image may serve as legal evidence.

The major breakthrough with this new system is the compression of the biometric features for identification purposes to a few hundred bytes. The FRR has been determined to be less than 0.5%. However, the FAR corresponding to this level has not been released. If this new ATM technology is introduced throughout the banking world it will have a major impact on the biometric identification industry and will lead to wider acceptance by the general public.

A facial recognition system, FR1000, which can verify a person even in the dark has been released recently by Technology Recognition Systems. This system uses an infrared camera to capture a thermal image of the face. Differences in temperature between blood passing through veins and arteries within the face and the surrounding tissues are captured. In particular the shape and position of hot spots is used for verification. Although the actual temperatures change, making the hot spots contract

or expand, research has shown that the vascular pattern stays the same, as does the position of the hot spots in relation to each other. Information from the ears and nose are however discounted as they are the most susceptible to temperature change.

The enrollment process involves the capture of three images which are stored as a template. A PIN is also allocated to the user. On entry of the PIN the cameral automatically tilts so it is positioned correctly. As the tolerance of the camera angle is less than five degrees a light just above the camera ensures that the user's face is correctly positioned. The user is also required to stand a fixed distance so that they are in focus. The tolerance allowed is approximately 30 cm. With the assistance of the PIN the thermal image is compared with the library template for verification. The current system is expected to sell for around $65 000 Australian dollars. At this level it is anticipated that the system would have a limited market initially. The major cost is the thermal camera which only 5 years ago was sold for 1 million dollars. The costs are still dropping and the company expects that the system will eventually become available at under US$2000. In conjunction with the FR1000 system a much cheaper system, FR500, is expected to be released later in 1996 using conventional lighting.

Eye Patterns

Two commercial systems are currently available which use the blood vessel patterns on the retina and the structure of the iris respectively.

Eyedentify Inc, Baton Rouge, La., produces a retinal scan product which has been commercially available since 1985. Retinal scans involve a weak infrared light which is directed through the pupil to the back of the eye. The retinal pattern is reflected back to a CCD camera which captures the pattern. After processing the template consists of less than 100 bytes of information. Retina scans are one of the best performers on the market with low FRR and nearly 0% FAR. The system which sells for approximately $ 6 000 Australian dollars is in use in security access control in a range of military and bank facilities. A major problem with this technology is the user reluctance to place their eye against the camera for several seconds.

A device that examines the human iris has recently been developed by IriScan Inc. Mount Laurel, N.J. It has been observed that every iris has a highly detailed and unique texture that remains stable over decades of life. Observable features include contraction furrows, striations, pits, collagenous fibres and filaments. In fact the iris features exhibit more characteristics than the fingerprint and appear to be unique as the fingerprint. With the IrisScan system involves the video input of the iris image and the analysis of features in set zones. A 256 byte template is obtained for comparison. An advantage of this system over the retinal scan is that scans can be obtained from up to a metre away from the user.

Further research is being undertaken in the area of iras scans for specialist applications. A new start-up company called Sensar, Inc is developing iris-based biometrics for financial market application. In particular Sensar hopes to demonstrate an ATM -compatible device in the near future. The iris template would be stored on a magnetic stripe or in a future smart bank card chip.

Voice Recognition

Perhaps the least invasive of the biometric recognition technologies and the most natural to use is voice recognition. All of the systems that have been developed for voice recognition are based in more broadly based speech processing technology. Several large organisations such as AT&T, Bell Communications Research, Texas Instruments and Siemens have developed verification algorithms for telephone applications. In addition there have been a number of smaller companies that have focused on voice recognition for access control. Currently there are 13 voice recognition products available commercially with a further 11 under development.

There are two approaches to voice recognition. One approach is the use of dedicated hardware and software at the point of access. The second approach is to use networked PC based systems which can be linked to a telephone system. Common to these systems is the digitising of samples of speech, quantification and normalisation for time variation to yield time invariant features such as pitch, speed, energy density and waveform. This frequency domain analysis of speech has to date been almost exclusively applied in an attempt to extract a set of statistical biometric features associated with the voice of a particular speaker. The speaker is required to repeat, from 4 to 8 times, a reference set of words over a microphone or telephone at the enrollment stage. A voiceprint is then obtained by comparing the wave forms. In addition, a range of acceptable waveforms can be determined for the individual concerned. The voiceprint template varies from 24 bytes to 1KB which can be stored in a central database or smart card. Currently voice recognition systems are being used for physical access, ATM access, computer access and home confinement.

The current systems suffer form a number of serious limitations associated with , for example, tedious enrollment procedures, high computational complexity, and a vulnerability to artifacts such as background noise. For example the SpeakerKey Voice Verifier system produced by ITT takes 4.5 minutes for enrollment and 20 seconds for verification. Despite this the system produced a FRR-FAR crossover of 1.7% for a test of 187 people which compares favorably with the facial recognition system.

A major problem with voice recognition systems is the wide variability of speech patterns for an individual and the perceived opportunity for impersonation. Fortunately the hazard of impersonation is not great as the systems purposely focus on characteristics of speech other than those that people listen to and imitate. A more serious concern is however the false rejection of individuals due to changes in voice patterns relating to such things as colds and background noise and the problem with discriminating siblings and twins. A great deal of research is being undertaken to improve the current systems including the use of Artificial Neural Networks and Hidden Markov Fields for processing. One system being developed by Domain Dynamics Limited and Cranfield University which uses a new simplified digital language and neural network combination is proving highly effective and can handle different background noises and can recognise high quality recordings from live speech [4].

Signature Dynamics

Considerable development has taken place in the area of signature dynamics with its promise of automating the job of verifying signatures in the financial community. Over 100 patents have been issued in the field including several for IBM, NRC and Visa. The 10 products that are available commercially rely on different aspects of the dynamic process of making a signature. These include the speed of writing, the order of strokes and flexible pattern matching using neural networks. While forgers may produce good geometric replicas there is likely to be significant timing variations. The user initially enrolls by entering several signatures. Generally, this is done with wired pens or sensitive tablets.

The key in signature recognition is to distinguish between habitual patterns and those that vary with almost every signature. In addition the system has to allow for variability in consistency of the user. One system that has undergone extensive testing before being released on the market is the Countermatch system developed by AEC Technology in England [7]. This system uses neural networks to create the signature template and the acceptable variation. A user who is more consistent in their signature pattern will have a template which will allow less variation on the acceptable signature than a user with a sloppy variable signature. During 1994 the system was trialled with the Employment Services in the UK for the fortnightly collection of unemployment benefits. As with PIN numbers the users where allowed three attempts at signing on. Approximately 48 000 signature attempts were recorded with 98% of the sign-ons being accepted and 94% requiring one signature attempt. Of the rejections, approximately 2-3% were directly attributable to the matching algorithm. The system was accepted by both the Employment Service and the users and has shown to have a deterrent effect as well as reducing clerical errors.

The financial industry to date has been reluctant to adopt the systems due to unacceptably high false rejection rate. Despite this it is expected that with improvements such systems will be common place wherever signature verification and checking is required.

Keystroke Dynamics

Keystroke dynamics, also known as typing rhythms, is currently undergoing significant research. This method analyses the way a user types at a terminal by monitoring the keyboard inputs. Studies have been undertaken establishing that typing patterns are unique to a typist. However it was observed that poor typists show greater variation and are therefore harder to identify.

The greatest application is in computer security to identify the user at the terminal. The advantage of keystroke dynamics is that neither enrollment or verification disturbs the regular work flow. Since the input device is the existing keyboard costs are kept to a minimum. Despite this the few attempts at a commercial product have failed due to technical problems with the physical characteristics of the keyboard and communication protocol structures.

Comparison of Biometric Identification Systems

The choice of a biometric identification system will depend on many factors. Important factors include the cost, size of device, size of template ,ease of use, user and operator training, invasiveness, FRR-FAR level requirements and the suitability of biometric for the specific application.

Comparison studies of biometrics have been undertaken by a number of government agencies. For example, in coordination with the an internal research department, the National Security Agency of the United States Department of Defence undertakes regular investigations to determine the biometrics which are appropriate for use in their environment [1].A recent summary of their results is given in the following table:

Biometric Technology	Operator Training	User Training	Ease of Use	Invasiveness	Template Size
Hand Geometry	minimal	minimal	easy	moderate	9 bytes
Retinal Scanning	moderate	extensive	hard	extensive	< 100 bytes
Speech Processing	minimal	moderate	moderate	minimal	~ 1000 bytes
Fingerprint	minimal	moderate	moderate	moderate	~2000 bytes
Face Recognition	moderate	minimal	easy	none	~ 2000 bytes
Weight	minimal	none	easy	none	4 bytes

Table 1. Biometric Devices

The Department used this information, for example, to determine the most appropriate biometric for use in automated visitor centres at strategic sites. The initial implementation of a biometric for use with an automated visitor centre was based on the requirement to restrict access to sensitive areas and to use the device that had the best false acceptance and rejection rate at the time. In implementing the visitor centre it was decided that a biometric was required that was not only perceived to be non invasive but was easy to train the average operator and end user. Also the biometric had to be a product that had been on the market for several years with known weaknesses and strengths. Based on this criteria it was decided to accept the ID3D HandKey system which fell within the acceptable FRR and FAR for the application. Similarly this system has been accepted as the US Department of Energy standard biometric technology and device. With rapid changes in biometric technology and their features the table and hence the choice of biometric technology require regular update.

Specific advantages and disadvantages for each of the biometric technologies are summarised as follows.

Biometric Technology	Advantages	Disadvantages
Fingerprints	Size of sensor Low FAR Stability and uniqueness of features	User reluctance Variation in image quality
Hand Geometry	Balanced FRR-FAR Small template size	Size of sensor
Face	User friendly	Variability of user Moderate FRR-FAR
Eye	Good FRR-FAR Stability and uniqueness of features	User reluctance Bulky and expensive
Voice	User friendly	Moderate FRR-FAR Variability of user
Signature	User friendly	Poor FRR Variability of user
Keystroke Dynamics	User friendly	Experimental

Of the systems currently available the fingerprint and hand geometry biometrics have the greatest share of the market. In many areas the fingerprint system is popular. While there is an initial reluctance of users to use the system, due to criminal connotations, this appears to be changing. A pilot program is being conducted at Toronto Airport by the United States Immigration and Naturalisation Service where frequent travelers have the option of presenting either their fingerprint or hand as a biometric identifier. Four hundred and four people selected fingerprints while only fourteen selected hand geometry system [13]. Recently a report to Congress recommends fingerprint technology as the most viable option for Electronic Benefits Transfer because trials have shown that it has been universally accepted and has proven to be reliable.

Despite fingerprint and hand geometry dominating the current biometric market it can be anticipated that there will be niche markets for each of the biometrics. The biometrics based on behavioral and face characteristics have the greatest potential for growth if the variability problem can be overcome.

Future Applications

While access control to strategic facilities has been the major application of biometric identification there is a much larger range of applications yet to be realised. One such application is the use of biometric identification for securing electronic data and financial transactions. In 1993 the Audit Commission in the United States conducted a survey to determine the amount of computer abuse in the public and private sector.

The commission found that, since 1990 survey there had been a threefold increase in the number of reported incidents, a 38% increase in the number of frauds and a 183% increase in the total value of the reported incidents [6].

With the growing number of data and financial transactions there is an urgent need to secure such transactions from theft and fraud. Examples include electronic home shopping via the internet, banking on PC's to a range of on-line information services, public and private databases and data stored locally on a computer. Despite sophisticated encryption algorithms the systems can be compromised by someone who knows the key. The problem is that forms of identification which are based on something possessed or known can be compromised and are transferable to other users. ID cards, passwords, encryption keys and PIN's can all be lost, stolen or transferred. By using biometric technology the true identity can be verified thus providing a higher level of protection. It is expected that with the introduction of advanced card technology and the capability of incorporating biometric information there will be much wider acceptance and use of biometrics. Applications in the data and financial transactions area are numerous. Listed below are some of the applications in which biometrics can be used [17]:

Electronic Transactions
- Paper-less transactions
- Cash-less transactions
- Remote banking
- Securities trading
- Credit and debit cards

Computer, database and network security
- Individual computer authority
- Remote computer authority
- Network authority
- Database authority
- Individual file authority
- On-line service authorisation

Credential authorisation
- Proof of age
- Driver's license ID
- National ID cards
- Registered Voter ID
- Citizen ID and passports
- Doctor ID
- Patient ID
- Employee ID and badges
- Customer ID
- Benefit recipient ID

While the banks have been slow to introduce the technology for fear of loosing customers it is expected that with greater user acceptance of the technology, lowering costs and most importantly acceptable FRR levels there will be significant growth in the next few years. Such systems will significantly reduce bankcard fraud which is a major problem today.

An example of what is to come in the computer industry is given by the Oracle database system where a new secure service option has been announced which will involve the user providing fingerprint verification via an Encrypted Verification Terminal before access to the database is granted. This security scheme will guarantees that all database accesses from unsupervised or remote locations are made by authorised personnel only and that any false attempts will be logged for further investigation.

A major application of biometric identification in the near future is the use of biometrics for the identifying benefit claimants. This has become a major issue in the United States as state and federal authorities seek to curb fraud and cut administrative costs.

Currently close to US$500 billion per year is issued in the United States to claimants of social security, railroad retirement, federal civilian retirements, military pensions, food stamps and women, infants and children's benefits. Fraud relating to benefits is estimated to be currently as high as 10%, or US$50 billion. With such a large problem there is an obvious need to improve the identification of claimants. In 1994 the Federal Electronic Transfer Task Force proposed that federal benefits should be dispensed by electronic means in all states by 1999. States are being encouraged to consider innovative technologies such as biometrics.

At the state level a lead is being set in New York where a system to replace paper based food stamps with cards carrying a fingerprint has been approved. A pilot project, run by the Department of Social Security, will begin in 1996 where claimants will use their cards with their fingerprints to verify their identity at retail outlets. There is already evidence of the savings on fraud. In San Diego county, California which implemented fingerprint recognition for welfare claimants over US$220 000 was saved in the first 6 months including US$180 000 from general relief payment and US$40 000 from the food stamp programme. This evidence, which is expected to be realised in other trials, will hasten the introduction of biometric technology in the welfare system both in the United States and throughout the world.

A further application that is likely to gain wider acceptance in the near future will be the use of biometric verification by customs and immigration. With the increasing movement of people around the world and the need to improve the processing speed at customs and immigration there will be a shift towards automated systems and improved methods of verification for low risk passengers. Unfortunately passport fraud has also become a major concern in some countries due to stealing and tampering of documents. With the use of biometric templates incorporated in a card, passport or boarding pass there is a solution at hand. Trial studies are currently being undertaken at a number of airports where, for example, frequent flyers have volunteered to enroll and use the biometric in return for quick processing upon

verification. Projects include INSPASS in the united states, CANPASS in Canada. Australia, Singapore, Hong Kong, Holland, Germany, and the United Kingdom are actively developing automated inspection systems. The choice of the best biometric and management system are yet to be determined. The INSPASS system uses hand geometry while the systems in Canada and proposed for Singapore will use fingerprints. A facial recognition system is currently under testing at Adelaide. Other countries will be using hand geometry or a combination of hand geometry and fingerprints. High level discussions have already started between countries in an attempt to identify appropriate standards for the future. Already the same card used for CANPASS can be used for INSPASS after the person has enrolled on both systems.

With the increasing number of stolen vehicles and associated costs there has been considerable interest recently by vehicle manufactures and insurance companies to develop improved car security systems. One area that is of interest and is currently undergoing research in Australia is the use of biometrics to identify the owner or designated drivers of the vehicle. For example, scanners imbedded on the dash, steering wheel or door handle have the potential to provide the maximum level of protection required.

Future Issues

With the wide spread use of biometric identification systems in the public sector for such things as welfare payments and immigration and customs control there will be a need to develop appropriate standards for the type and use of the system. This will also be true if ,for example, the financial institutions wish to allow their clients to use biometric readers at retail outlets. Currently there is evidence that different states in the United States may trial different systems for welfare payments. This will initially lead to a lack of portability between states but will provide relevant data for the choice of a widespread standard at a later stage.

The established biometric companies such as Identrix and Recognition Systems are already involved in lobbying for their system to be the standard. It is belief of these established companies that as biometrics become more common in everyday use and standards are set for the industry, only a few technologies and companies will survive [17]. While it can be expected that many biometric companies will fall by the wayside it is being over simplistic to assume that there will be only one standard. It is likely that different standards will be set for different applications and there will still be many stand alone applications where standards will not restrict the type of biometric technology to be used.

The immigration authorites of Australia, Bermuda, Canada, Germany, Holland, the United Kingdom and the United States have already been working for the last year to develop a standard for automated inspections. This includes design of the technological platform to ensure that the card will have a useful life of approximately 5 years and is likely to be operated by the private sector.

A second issue will be the best integration of biometric technology with the advanced card technology. The advanced card technology is currently undergoing substantial

innovation. During the next five years we will see the advanced cards and security technology increasingly used in a broad range of applications including telecommunications, banking, home interactive services, health care and welfare. With the increase in memory and data storage and the possibility of combining functions on the advanced card there will be need to determine the best way to integrate and use biometric templates within the card. The opportunity will be available to use the biometric template in the card not only for access control but also as an encryption key for electronic transfer of data and information. This may enable, for example, a secure electronic voting system to be established where, for example, the voter's identity can be assured and yet where the authorities can also be assured that the voter has made only one vote. A great deal of research has yet to be undertaken before such issues can be resolved.

A third issue will be the best integration of the biometric system with other security components as part of the total security plan for a facility. Research will need to be undertaken relating not only to the technological interface but also the human - technology interface. For the biometric system to be truly effective there will be a need for training of personnel including the enrolled users, security technicians and security managers and the inclusion of audit and system report functions.

Conclusion

This paper has painted a rosy picture for the biometric identification industry. Substantial growth is assured with more reliable, user friendly and lower cost systems. This growth will be linked to the growth in advanced card , communication, computer and other electronic technologies. Substantial research is underway to provide for improved biometric systems, to develop systems for specialist applications and to integrate developments with related technologies.

References

[1] Carback, R.T. (1995) *Reducing Manpower Intensive Tasks through Automation of Security Technologies* Proceedings of the IEEE International Carnahan Conference on Security Technology , *331-339*

[2] Cross, J.M. and Smith C.L. (1994) *Thermographic imaging of the subcutaneous vascular network of the back of the hand for personal identification.* Proceedings of the Security Research Symposium, Griffith University, Queensland.

[3] Cross, J.M. and Smith C.L. (1995) *Thermographic imaging of the subcutaneous vascular network of the back of the hand for biometric identification.* Proceedings of the IEEE International Carnahan Conference on Security Technology , *20-35*

[4] George, M.H. and King R.A. (1995) *A robust speaker verification biometric* Proceedings of the IEEE International Carnahan Conference on Security Technology , *41-46*

[5] Hawkes, P.L. & Clayden, D.O. (1993, September). *Veincheck research for automatic identification of people.* Paper presented at the Hand and Fingerprint Seminar at NPL.

[6] Hulford, C. (1995) Opportunity Makes a Thief. *Secure Computing*, pp. 27

[7] Lewcock, A. (1995) *Computerised Signature Verification* Proceedings of the IEEE International Carnahan Conference on Security Technology ,*72-78*

[8] MacGregor, P. & Welford, R. (1991). Veincheck: Imaging for security and personnel identification. *Advanced Imaging, 6*(7), 52-56.

[9] MacGregor, P. & Welford, R. (1992). Veincheck lends a hand for high security. *Sensor Review, 12*(3), 19-23.

[10] Mehnert, A.J., Cross, J.M, Smith, C.L., & Chia, K.L. (1995) *A personal identification biometric system based on back-of-hand vein patterns.* Technical Report, Australian Institute of Security and Applied Technology, Edith Cowan University, ISBN:0-7298-0193-4

[11] Mehnert, A.J., Cross, J.M., & Smith, C.L. (1995). *A Novel Biometric: The Vein Pattern on the Back of the Hand,* Proceedings of the Second National security Research Symposium, Edith Cowan University, Western Australia

[12] Miller, B. (1994). Vital signs of identity. *IEEE Spectrum, 31*(2), 22-30.

[13] Newman,E. (1995) *Survey: So what do people think of biometrics?* Biometric Technology Today 3. 7-8

[14] Parks, J.R. (1991). *Personal identification – biometrics* in Lindsay, D.T. and Price, W.L. (Eds.) Information security, pp. 181-191. North Holland: Elsevier Science Publishers.

[15] Sagar, V.K., Ngo, D.B.L. and Foo, K.C.K. (1995) *Fuzzy Feature Selection for Fingerprint Identification* Proceedings of the IEEE International Carnahan Conference on Security Technology , *85-90.*

[16] Simpson, L. (1994). The Fingerscan personal ID system. *Silicon Chip, 7*(5),8-9.

[17] Stockel, A. (1995). *Securing Data and Financial Transactions.* Proceedings of the IEEE International Carnahan Conference on Security Technology ,*397-401.*

[18] Vuori, T.A., and Smith, C.L. (1995) . *Biometric Imaging: Three Dimensional Imaging of the Human Hand using Coded Structured Lighting,* Technical Report, Australian Institute of Security and Applied Technology, Edith Cowan University ISBN: 0-7298-0195-0.