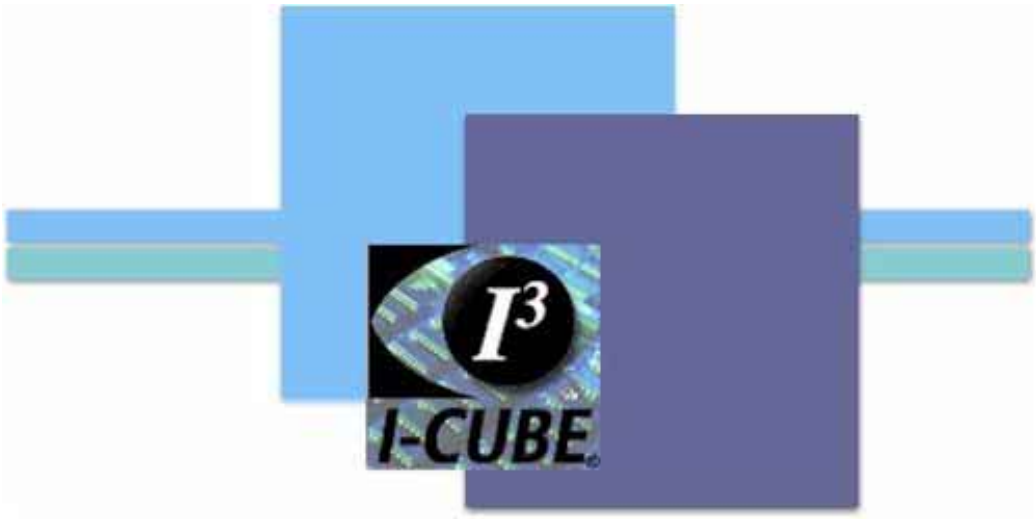
ACCESS CONTROL VERIFIED BY FACIAL RECOGNTION

For

The Smart Card Society of Southern Africa cc, JHB, South Africa



BY

B. T. DUDLEY

MBA (Information Technology, UND) MSc (Image Analysis, UNP, Cum Laude)

7-8 June 2004

Table of Contents

List of Figures

List of Tables

Abstract

Biometric security should be seen as an extension of human intelligence, and not as a replacement for it, because automated security will only be as good as the human intelligence that backs it up. The danger of relying too heavily on technology is nowhere more real than in the area of biometric access control. Such access control is most effective if the people you are trying to locate are aware of its use. Audit trails left by an individual as he or she uses doors, turnstiles, computers and any other services that require biometric authentication (i.e., possibly any activity that requires the use of a card) could become a significant contribution to intelligence systems.

Companies engage in a constant battle to detect and prevent illegal access to premises and to ensure that the person using the access card is actually present and can be verified as the person issued the card. In order to overcome the problems associated with illegal access, loss prevention directors must possess accurate information regarding the access to areas where the loss might occur, as well as a way to identify and track employees. Implementing biometric face recognition linked to access cards will allow this to occur. The Veraport system described below uses the Acsys HNet advanced face tracking and recognition technology to provide the ultimate in non-intrusive biometric access control allowing:

- **Dual biometric capability – can be implemented in a number of different combinations: Card + Face; Card + Face + Finger; Card + Face + PIN; Card only**
- **Streamlined enrollment procedures – soft enrollment eliminates delays, permits addition of users even if client is disconnected from server; new images added for template update during normal operation; images filtered for maximal pattern variation; heuristic scripting of interactive enrollment speech/text**
- **Improved image processing – dual image filtering**
- **Reduction in template size – a templates occupies only 15KB**
- **Template encryption – templates can be encrypted**

Acsys Veraport provides a complete, user-friendly access control solution for small- to medium-scale facilities - up to 200 access points and 20,000 users.

Introduction

"Biometric" technology, and specifically face recognition, which can recognize people from a facial image, is becoming cheaper and more powerful as technology improves. Biometrics comes in many forms. The idea is said to date back to ancient Egypt, when records of distinguishing features and bodily measurements were used to make sure that people were who they claimed to be. Modern computer based biometric systems are employed for identification ("who is this person?"), in which a subject's identity is determined by comparing a measured biometric against a database of stored records a one to many comparison.

Technology	Acquisition Device
Fingerprint	Chip or reader embedded in turnstile
Voice recognition	Microphone
Facial recognition	Video camera, surveillance camera, single-image camera
Iris-recognition	Infrared-enabled video camera
Retina-recognition	Wall-mountable unit
Hand geometry	Proprietary wall-mounted unit
Signature-recognition	Signature tablet, motion-sensitive stylus
Keystroke-recognition	Keyboard or keypad

1 Acquisition devices associated with biometric technology

Despite vendor claims, there is no “ideal” biometric technology, although examples of successful uses exist. Facial recognition, a technology that has gained ground in recent years thanks to the falling price of computer power. It works by analysing a video image or photograph and identifying the positions of several dozen fixed "nodal points" on a person's face. These nodal points, mostly between the forehead and the upper lip, are only slightly affected by expression or the presence of facial hair.

Facial recognition is becoming more widespread, because it can exploit existing cameras and existing databases of facial images from driving licences and passports. Exclusion techniques based on BIOMETRICS have some serious technological advantages. If a single positive identification can prevent a theft, then the sooner one begins to use the technology the better. Yes, exclusion systems are capable of achieving the success rate necessary for those kinds of decisions. For the most part, biometrics appears to be a technology whose time has come from the marketing viewpoint. It is suggested that the biometrics be used as a TOOL, which is used to COMFIRM identity, so not as the primary identification (Business Week, 2003 Why Biometrics Is No Magic Bullet Available online at**: http: //www.businessweek.com/technology/content/ jul2003/tc20030722_2846_tc125.htm).**

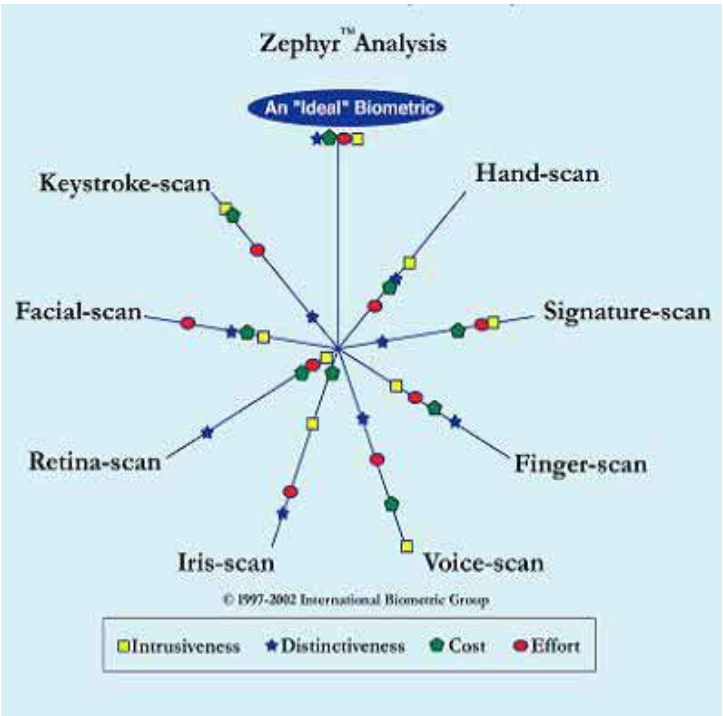


Figure Zephyr Analysis to determine the “ideal” biometric

There is no doubt that CCTV is fast becoming an important tool in the fight against illegal entry. Statistics point to major reductions in the amount of illegal entry, abuse of access control and preventing ghost workers where cameras are installed. When it comes to protecting your property, there is nothing better than having the ability to link a face to an access card and deter potential criminals.

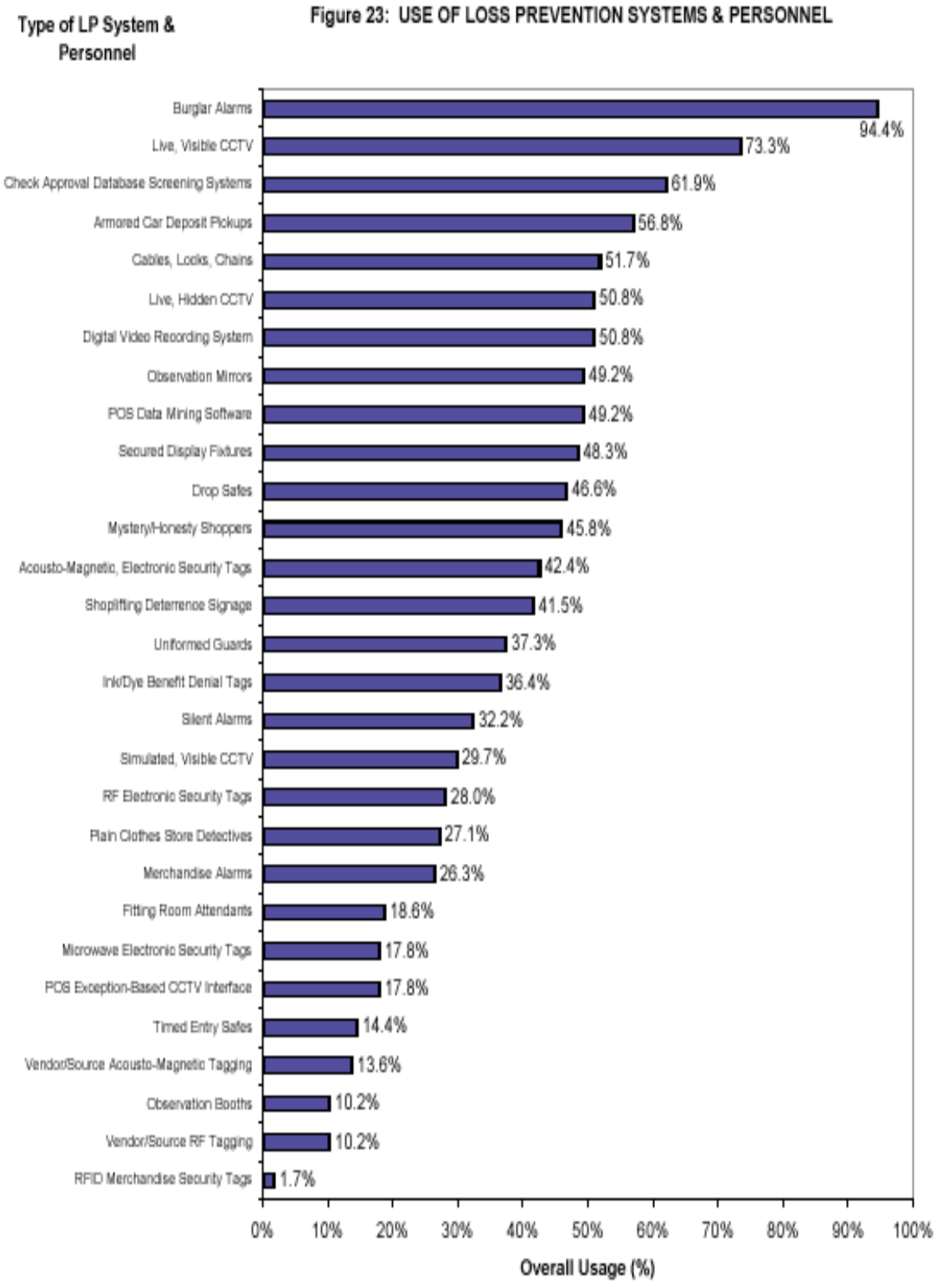


Figure Use of CCTV systems is on the increase.

THE THEORY BEHIND USING FACE RECOGNITION FOR ACCESS CONTROL

New real time security alternatives are a reality today with lighting fast Face Recognition System.

Face recognition used for access control and logging via a PROX CARD. Exclusion techniques based on BIOMETRICS have some serious technological advantages. If a single positive identification can prevent a theft, then the sooner one begins to use the

technology the better. Yes, exclusion systems are capable of achieving the success rate necessary for those kinds of decisions. For the most part, biometrics appears to be a technology whose time has come from the marketing viewpoint. It is suggested that the biometrics be used as a TOOL, which is used to COMFIRM identity, so not as the primary identification **(Business Week, 2003 Why Biometrics Is No Magic Bullet Available online at: http: //www.businessweek.com/technology/content/jul2003/tc20030722_2846_tc125.htm).**

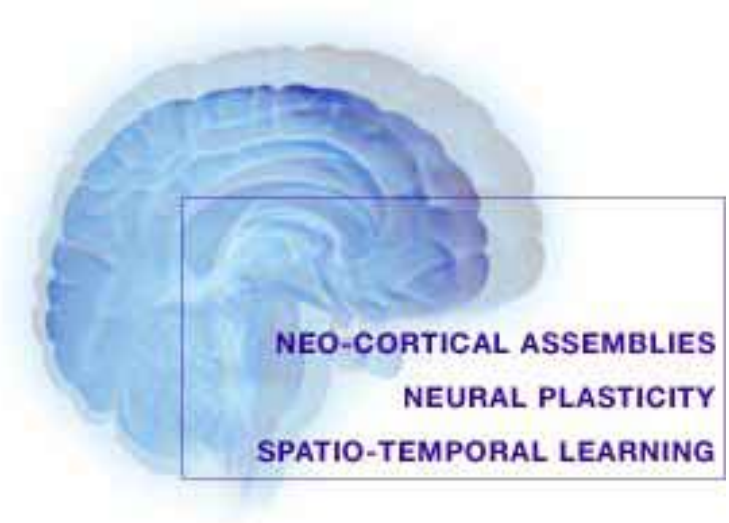
Introducing the exciting new field of **Biomimetic Intelligence.**

AND Corporation is the provider of **Application Development**

Services, Software Systems and **Licensor** of this breakthrough technology.

Overview

Biomimetic Intelligence is the science of understanding and replicating the processing mechanisms and structure of the brain. Traditional neural networks have little or no resemblance to actual neurological structures, and more importantly, have proven to be very limited in capability. The HNeT technology, however, applies the power of digital holography within synthetic neuron cells. Assemblies comprised of such cells have one-to-one correspondence with the primary cell structures of the brain. These biomimetic structures provide the capability for truly real-time learning, and present a vast increase in (stimulus-response) memory storage capacity.
To provide a practical example, a cell assembly can locate and track human faces in real time. A cell assembly can learn facial images in real time, building within its memory all observed forms of an individual, and subsequently identify that individual within a crowd, even determine facial expression such as smiling or frowning, etc. This application is at the upper limit of technological capability when employing traditional methods. Application of the basic two-cell "cerebellar" model reduces the above task to a rather straight-forward procedure. The HNeT technology is not limited to face tracking / identification, but may be similarly applied to numerous areas within the medical sector, process control, automation, defence, financial, etc.



HNeT Tools

The HNeT system allows our developers to construct neuron cell assemblies, and integrate these neural assemblies into applications. The core of the HNeT system is a Dynamic Link Library (DLL) containing over 90 functions for creation of cell assemblies, and customization of cells. Employing holographic principles, HNeT cells provide both real-time learning and dramatic improvements in performance over structurally more complex back-propagation / genetic neural networks. Holographic / quantum neural technology provides an exceptionally high "connection per second" or CPS rating; in excess of 40 Million CPS on Pentium III processors. This allows an HNeT cell assembly to learn and respond to several thousand input patterns in under a second.

The SL Platform **(a non-programmers interface) provides for training and designing supervised feed-forward cell assemblies cells from ASCII or binary files. The following provides a general specification list for the HNeT2000 Application Development System.**

Performance Features

The following details some of the performance features that are unique to the HNeT technology. The most basic cell assembly (based on the cerebellar model) is comprised of two synthetic neuron cells (granule and Purkinje). The performance aspects discussed are also characteristic of larger and more elaborate cell assembly structures within HNeT, these more advanced structures providing further extensions to the core operation (i.e. neo-cortical model, temporally based learning, and unsupervised hyperincursive models).

A brief summary of the following performance features are covered:

General Comparisons	**Provides general performance characteristics pertaining to learning speed and accuracy, with comparisons to traditional neural networks**
Convergence	**Illustrates the learning convergence characteristics that occur when learning over multiple training exposures or epochs**
Generalization	**Concerns aspects concerning generalization and interpolation of the stimulus-response mapping**
Neural Plasticity	**Describes the process of neural pruning and re-growth, and illustrates performance gained through the resultant optimization of input combinatorics**

General Comparisons

The two cell cerebellar model within HNeT is compared against a commercial system based on traditional genetic neural networks. The genetic neural network used in this comparison permits up to 2 hidden layers, and accommodates 256 cells per layer. The primary feature of this type of neural network is the genetic based search used to find the "optimal" configuration (i.e. number of cells, hidden layers, interconnections, etc).

The holographic / quantum neural approach (HNeT) does not require a search process, and learns many orders of magnitude faster than traditional back-propagation or genetic based neural networks.

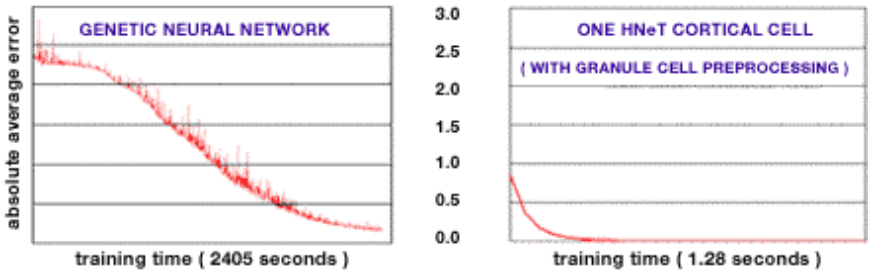
The Monte Carlo Test

Accepted by many neural network experts as one of the more rigorous tests when it comes to evaluating artificial neural systems. In a Monte Carlo evaluation, the stimulus-response patterns are comprised of random numbers. The comparisons below use 5 input variables for the stimulus and one response variable, with values uniformly distributed between 0.0 and 10.0. The learning / convergence characteristics are shown for densities of 100, 500, and 1000 stimulus-response patterns respectively. At these low pattern storage densities, non-linear capabilities of traditional back-propagation and genetic neural networks are pushed beyond their limit.

Applying this standard test method, one may evaluate three aspects of operation. The first aspect concerns the stimulus-response memory capacity of the system, the second concerns the recall accuracy of the trained cell, and the third concerns learning speed. All three performance figures are shown for a 160 MHz Pentium II.

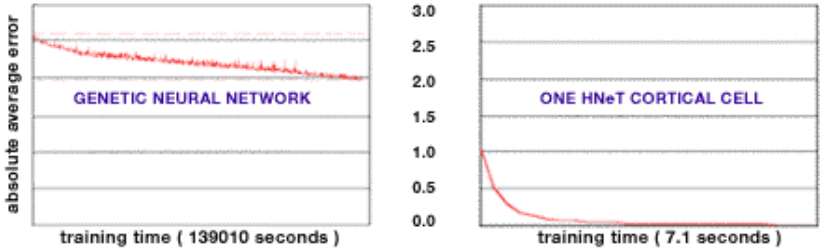
Comparison 1 – Learning 100 Stimulus-Response Patterns

After the initial genetic search, training time applied to the genetic neural network is 40 minutes. By comparison, training time for the HNeT system is 1.28 seconds. At a storage density of 100 patterns the HNeT granule-cortical cell structure is 100 times more accurate and 2000 times faster than the traditional neural network.



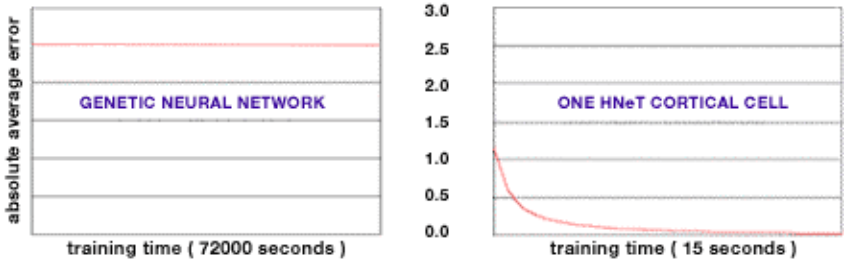
Comparison 2 – Learning 500 Stimulus-Response Patterns

Increasing the number of stimulus-response patterns causes the genetic neural network to approach a state of saturation. At this level of storage density, traditional neural networks break down. Learning capacity of the HNeT granule-cortical cell combination is unaffected by the increase in storage, and displays a convergence similar to the test involving 100 patterns.



Comparison 3 – Learning 1000 Stimulus-Response Patterns

At 1000 stimulus-response patterns the genetic neural network is unable to achieve any measurable level of convergence, even after 20 hours of training. The rapid learning characteristic of the



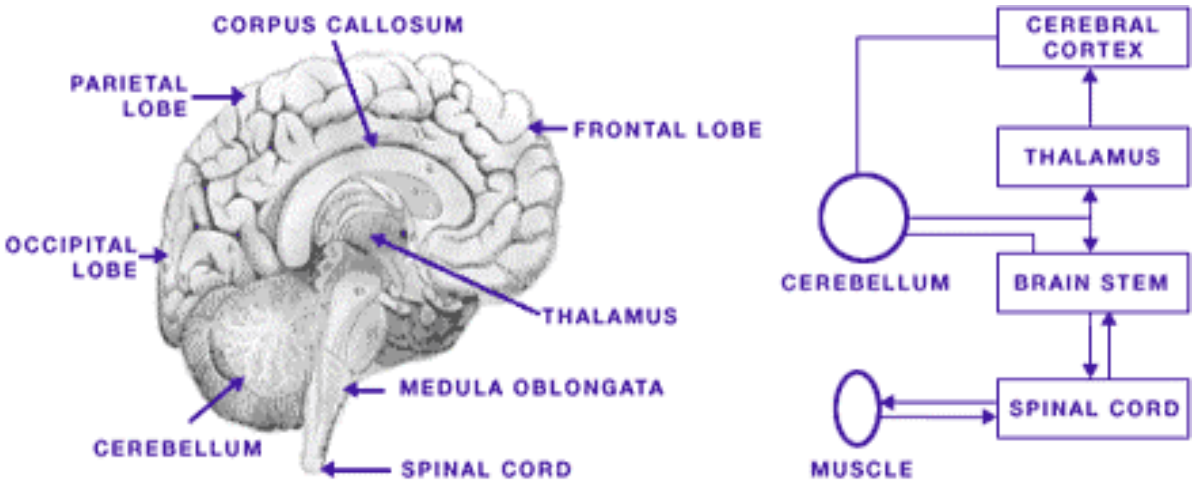
HNeT system is again unaffected by this increase in storage density.

The Biology

The following provides an overview of HNeT biomimetic intelligence. Biomimetic intelligence models cell inter-connectivity and signal processing aspects of actual neuron cell assemblies within sections of the brain referred to as the neo-cortex (gray matter or outer layer), the cerebellum (near the base of the brain) and the hippocampus. The HNeT system allows one to construct cell assemblies ranging in capability from supervised feed-forward systems, to more advanced spatio-temporal and hyperincursive models.

HNeT cells have been given biological names due to their similarity to specific classes of neuron cells (i.e. the granule, stellate / Martinotti, pyramidal, and Purkinje cells).

This section is provided for a more technically inclined audience. Although the mathematical basis for HNeT is somewhat abstract, one does not require an in-depth understanding of the theory in order to design and build applications using the HNeT2000 Application Development System. It is important that one understands how stimulus-response information is presented to the system, and how the various types of holographic / quantum neural cells interact with each other.



A stimulus-response pattern or "memory" may be represented by a set of values, reflecting conditions or states measured within an external environment, such as pressure, temperature, brightness, etc. During stimulus-response learning, neural cells associate or "map" one set of analog values (i.e. the stimulus fields) to an associated set of values (i.e. the responses). When the stimulus is distributed over a time span, one has spatio-temporal learning.

The mathematical basis for HNeT permits vast numbers of stimulus-response patterns to be learned and superimposed (enfolded) onto a matrix comprised of complex scalars, called the cell's cortical memory. In fact, the number of values used to store cortical memory is often no larger than the number of values contained within a single stimulus pattern. The mechanism for holographic storage displays a capacity to achieve extremely high information densities, due to the fact that large numbers of stimulus-response memories can be enfolded onto the same set of scalars (in other words - computer RAM).

PRICACY DISCUSSION

Discussion concerning the implementation of large-scale biometric systems always include speculation concerning public attitudes. One of the difficulties with what is said about public attitudes, on any subject, is that interest groups tend to impute their own fears, values and biases to the public. Most of the interest groups, who speak out on the subject of privacy, tend to have attitudes that are not friendly to the use of biometrics. The danger is that the more those views are repeated, the more they will tend to shape public opinion. Although there is much talk in the biometric community about the public attitude, most who raise the point do so on a very superficial basis. There has been little organised dialogue or ongoing discussion concerning the subject of public attitude. It would be worthwhile study on attitudes and biases within the various segments of the biometric community, for and against large-scale biometric systems. Some do not see it within their business interest for there to be rapid progress toward large systems, since they may not feel that their technology or product is yet positioned to be competitive or dominant or are concerned that a niche they occupy or intend to occupy will be squeezed out by systems of more general application. Cf. Betamax vs. VHS; Mac OS vs. DOS vs. Windows, etc. The in depth study of the problems of privacy is beyond this study (see Westin, A, 2001 for more information).

New technology is boosting biometric surveillance (Grossman, 2003) and privacy may vanish forever. It is possible that legal and political issues such as privacy and data access could hinder the application of biometrics (Lee, 2003). Most of the public polls suggest that there is nowhere near the opposition to exclusion techniques that is claimed. Very little effort has been made by the government, the press or the exclusion industry to explain, and to distinguish, exclusion techniques from the controls that ought be placed on informational databases. The result is that public concerns on the collection, use and release of data are being largely ignored. Privacy concerns are very difficult to address, since they change over time, and differs across cultures. By adhering to applicable best practices, even those technologies more capable of being misused - primarily facial recognition and fingerprint - can be deployed in a privacy-sympathetic fashion (BioPrivacy Best Practices 2003 Available online at: http://www.ibgweb.com/ reports/public/reports

/privacy_best_practices.html). The use of the information gathered for exclusion purposes needs to be weighed against the possible use of the information. Fingerprint, face and iris have the highest privacy risk. It is essential that appropriate protection should be in place to ensure the technology is not misused (Mc Cullagh, D 2003). Self-reporting data would be wrapped in software or digital watermarks that guard against misuse of private information by tracking who has used the data, and where they have been moved (Roush, 2003). The manner is which proper protection occurs is beyond the scope of this study.

Identity theft, using stolen credit cards, phoney cheques, and other impostor scams to steal, is on the increase (Vijayan, 2003). Until recently, the only way to way to attack the problem has been to add expensive screening and administration procedures. However, steps such as hiring security guards, maintaining accurate databases, reviewing identity documents, and asking personal questions have proven to be costly, stopgap measures that can be defeated by enterprising criminals. Compared to other methods of proving identity, biometrics are the only tools that can enhance personal privacy and still deliver effective solutions in situations that require confirmation of identity.

Evaluation & Recommendations

VERAPORT

The Acsys Veraport uses our advanced face tracking and recognition technology to provide the ultimate in non-intrusive biometric access control. Acsys Veraport provides a complete, user-friendly access control solution for small- to medium-scale facilities - up to 200 access points and 20,000 users. Acsys Veraport's two-tier, client-server architecture can be inserted into existing access controls systems, and it can also be integrated with third party time & attendance solutions.

Client
The user-friendly, interactive client portion of the Acsys Veraport system provides enrollment and authentication services. Initial user enrollment is completely automated: the system directs the user where to stand and in which direction to look. The interactive enrollment procedure is based on preset heuristic scripting. Each client/access point can be configured independently to use different combinations of authentication factors (card, face, finger, PIN). Biometrics templates are cached locally so that verification can occur without a live connection to the Server.

Server
The Acsys Veraport server provides an easy-to-use Operator's Console for monitoring and responding to activity. The console allows an operator to monitor up to four access points simultaneously using streaming video. Alarms are annunciated automatically at the Operator's Console and optionally transmitted to remote devices using Wireless Local Area Network, Short Messaging System, and Wireless e-mail to help ensure that alarm events are dealt with in a timely and efficient manner. Audio and video feeds can be recorded digitally.

Database Server

Acsys Veraport supports Oracle 9i and all versions of Microsoft SQL Server databases. A database management utility is provided for viewing and editing the primary database, which is used to store templates, facial images, and user templates. User queries can be filtered by user group or last name, and can include wildcards.

Activity Monitoring and Recording

The activity log records all information pertaining to normal access events such as time, date, portal ID, event category (e.g., enroll/verify) as well as abnormal events or unauthorized entry attempts (e.g., enroll/verify failure, unregistered card, piggyback/tailgate detection). The system stores an image and logs each event for subsequent review or processing.
Please REVIEW the Acsys Veraport Feature Sheet (PDF) for more details.

PERSONAL ENTRANCE EXAMPLE

The person would walk up to the turnstile.

Swipe his access card and possibly enter his access code (possibly company number) via the reader, if required for EXTRA security.

By looking into the camera verification would occur, allowing the person to enter.

Figure Understanding who, when and what every person visiting the site is doing and very importantly, linking a FACE to a name allows one to control, limit and understand what people are doing on site. Something as simple as overtime or having the right people present can save the company thousands. This will not occur just be using a register or a access card.

Figure The ability to monitor who, when and with whom people exit leads to a greater understanding of the movement of people in the facility, leading to exception reporting, rather than routine reporting.

Figure The ability to enrol static images obtained from the DVR assists in speeding up the enrollment process. No longer can anyone gain access anywhere, real time monitoring now occurs.

Figure A fixed camera will be used to acquire the facial image.

Figure Example of the database images.

Figure The server manager, trainer and database.

CONCLUSION

The linking of an existing access card to the latest face access control technology provided by Acsys that will provide a tool via face recognition to verify a claimed identity of a person. The advantages of the NEURAL network are that the system leans over time and continually updates to take into consideration all lighting conditions and all changes in a persons makeup. This is assisted by the collection of numerous 3D images both during enrollment and during verification each time the user uses the system. The integration of cameras into the access control points will allow the movement of people to be monitored accuracy and effectively. We believe that the above solutions will grab the attention of all role players. Information Technology has become so integral to success that it is now not only a support function, but could plays a proactive and vital role in realising access control solutions. By combining access cards with CCTV and face recognition together these offer technology solutions and services that allow customers to efficiently integrate, manage and maintain their people, processes and assets.

Definitions

Active Impostor Acceptance **- When an impostor submits a modified simulated or reproduced biometric sample, intentionally attempting to relate it to another person who is an enrolee, and he/she is incorrectly identified or verified by a biometric system as being that enrolee. Compare with 'Passive Impostor Acceptance'.**
Algorithm **- A sequence of instructions that tell a biometric system how to solve a particular problem. An algorithm will have a finite number of steps and is typically used by the biometric engine to compute whether a biometric sample and template are a match. See also 'Artificial Neural Network'.**
Attempt **- The submission of a biometric sample to a biometric system for identification or verification. A biometric system may allow more than one attempt to identify or verify.**
Authentication **- Alternative term for 'Verification'.**
Automatic ID/Auto ID **- An umbrella term for any biometric system or other security technology that uses automatic means to check identity. This applies to both one-to-one verification and one-to-many identification.**
Behavioural Biometric **- A biometric, which is characterised by a behavioural trait that is learnt and acquired over time, rather than a physiological characteristic. However, physiological elements may influence the monitored behaviour.**
Biometric **- A measurable, physical characteristic or personal behavioural trait used to recognise the identity, or verify the claimed identity, of an enrolee.**
Biometric Application **- The use to which a biometric system is put.**
Biometric Data **- The information extracted from the biometric sample and used either to build a reference template (template data) or to compare against a previously created reference template (comparison data).**
Biometric Engine **- The software element of the biometric system, which processes biometric data during the stages of enrolment, capture, extraction and comparison.**
Biometric Device **- The part of a biometric system containing the sensor that captures a biometric sample from an individual.**
Biometric Sample **- Raw data representing a biometric characteristic of an end-user as captured by a biometric system (for example the image of a fingerprint).**
Capture **- The method of taking a biometric sample from the end user.**
Comparison **- The process of comparing a biometric sample with a previously stored reference template or templates. See also 'One-To-Many' and 'One-To-One'.**
Claim of Identity **- When a biometric sample is submitted to a biometric system to verify a claimed identity.**
Claimant **- A person submitting a biometric sample for verification or identification whilst claiming a legitimate or false identity.**
Database - **Any storage of biometric templates and related end user information. Even if only one biometric template or record is stored, the database will simply be "a database of one". Generally speaking, however, a database will contain a number of biometric records.**
End User - A person who interacts with a biometric system to enrol or have his/her identity checked.
Encryption - The act of converting biometric data into a code so that is it unable to be read. A key is used to decrypt (decode) the encrypted biometric data.
Enrolee - A person who has a biometric reference template on file.
Enrolment - The process of collecting biometric samples from a person, subsequent preparation and storage of biometric reference templates.
Enrolment Time - The time period a person must spend to have his/her biometric reference template successfully created.
Equal Error Rate - The error rate occurring when the decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances.
Extraction - The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.
Failure to Acquire - Failure of a biometric system to capture and extract biometric data (comparison data).

Failure to Acquire Rate - The frequency of a failure to acquire.
Failure to Enrol - Failure of the biometric system to form a proper enrolment template for an end-user. The failure may be due to failure to capture the biometric sample or failure to extract template data (of sufficient quality).
Failure to Enrol Rate - The proportion of the population of end-users failing to complete enrolment
False Acceptance - When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.
False Acceptance Rate/FAR - The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The False Accept Rate may be estimated as FAR = NFA / NIIA or FAR = NFA / NIVA where

FAR is the false acceptance rate
NFA is the number of false acceptances
NIIA is the number of impostor identification attempts
NIVA is the number of impostor verification attempts

False Rejection - When a biometric system fails to identify an enrolee or fails to verify the legitimate claimed identity of an enrolee.
False Rejection Rate/FRR - The probability that a biometric system will fail to identify an enrolee, or verify the legitimate claimed identity of an enrolee. The False Rejection Rate may be estimated as follows:
FRR = NFR / NEIA or FRR = NFR / NEVA where

FRR is the false rejection rate
NFR is the number of false rejections
NEIA is the number of enrolee identification attempts
NEVA is the number of enrolee verification attempts

This estimate assumes that the enrolee identification/verification attempts are representative of those for the whole population of end-users. The False Rejection Rate normally excludes 'Failure to Acquire' errors
Field Test / Field Trial - A trial of a biometric application in 'real-world' as opposed to laboratory conditions.
Filtering - The process of classifying biometric data according to information that is unrelated to the biometric data itself. This may involve filtering by sex, age, hair colour or other distinguishing factors, and including this information in the database .
Goats - Biometric system end users whose pattern of activity when interfacing with the system varies beyond the specified range allowed by the system, and who consequently may be falsely rejected by the system.
Identification/Identify - The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the enrolee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with 'Verification'.
Impostor - A person who submits a biometric sample in either an intentional or inadvertent attempt to pass him/herself off as another person who is an enrolee.
Live Capture - The process of capturing a biometric sample by an interaction between an end user and a biometric system.
Match/Matching - The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. An accept or reject decision is then based upon whether this score exceeds the given threshold.
Multiple Biometric - A biometric system that includes more than one biometric system or biometric technology.
Neural Net/Neural Network - One particular type of algorithm. An artificial neural network uses artificial intelligence to learn by past experience and compute whether a biometric sample and template are a match.
Performance Criteria - Pre-determined criteria established to evaluate the performance of the biometric system under test.
Physical/Physiological Biometric - A biometric which is characterised by a physical characteristic rather than a behavioural trait. However, behavioural elements may influence the biometric sample captured.

Population - The set of end-users for the application.
Recognition - The preferred term is 'Identification'.
Record - The template and other information about the end-user (e.g. banned)
Response Time - The time period for a biometric system to return a decision on identification or verification of a biometric sample.
Score - The level of similarity from comparing a biometric sample against a previously stored template.
Template/Reference Template - Data, which represents the biometric measurement of an enrolee, used by a biometric system for comparison against subsequently submitted biometric samples.
Template Ageing - The degree to which biometric data evolves and changes over time, and the process by which templates account for this change.
Template Size - The amount of computer memory taken up by the biometric data.
Third Party Test - An objective test, independent of a biometric vendor, usually carried out entirely within a test laboratory in controlled environmental conditions.
Threshold/Decision Threshold - The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.
Throughput Rate - The number of end users that a biometric system can process within a stated time interval.
Type I Error - In statistics, the rejection of the null hypothesis (default assumption) when it is true. In a biometric system the usual default assumption is that the claimant is genuine, in which case this error corresponds to a 'False Rejection'.
Type II Error - In statistics, the acceptance of the null hypothesis (default assumption) when it is false. In a biometric system the usual default assumption is that the claimant is genuine, so this error corresponds to a 'False Acceptance'.
User - The client to any biometric vendor. The user must be differentiated from the end user and is responsible for managing and implementing the biometric application rather than actually interacting with the biometric system.
Validation -The process of demonstrating that the system under consideration meets in all respects the specification of that system.
Verification/Verify - The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. Contrast with 'Identification'.
WSQ (Wavelet Transform/Scalar Quantisation) - A compression algorithm used to reduce the size of reference templates.

Appendices

Appendix I –DETAILED EQUIPMENT LIST.

Available on request

Face Recognition linked to a PROX CARD and / or PIN for ACCESS CONTROL:

Access control Face recognition for 500 people based on a single turnstile / door for a personal entrance including a fixed camera
See attached Excel spreadsheet.

VERAPORT SYSTEM DESIGN

ITEM	DETAIL	No. Required
VeraPort	**Includeds operators console and one client**	**1**
VOC	**VeraPort Operators Console (VOC) - Each additional system needs one**	**0**
Wiegand CB	**Wiegand to Serial Interface circuit board**	**1**
Digital I/O	**Digital I/O with relay circuit board**	**1**
	Stand alone circuit boards **Roughly 100 mm square** **Require 12 VDC power from some external supply** **Communicate to the host PC via RS 232 Serial port (Host PC must have 2 serial ports or some adaptor which can facilitate this.*)** **Employ unique communications protocol** **Use terminal blocks for most electrical connections. (Digital I/O is done directly off of circuit board traces and pads.)**	
PAL	**Portal Access License**	**0**
SERVER	**Where the client and server is on one machine**	**0**
CLIENT	**Where there are multiple machines add in clients**	**0**
Sup, Man & DB	**Support, Maintenance & Database -**	
	1-1000 users	**1**
	1001 - 5000 users	**0**
	5001 - 30 000 users	**0**
Frame Grabber	**Winnov's Videum 1000 Plus**	**1**

ITEM	DETAIL	No. Required

PC - Server	· Microsoft® Windows® 2000 Professional (Service Pack 3 or higher) or Microsoft® Windows® XP Professional (SP 1a) · 1.6 GHz Pentium 4 Processor · 512 MB RAM · 40 GB HDD · CD-ROM Drive · 2 RS-232C Ports · 16-bit SoundBlaster (or compatible) audio adapter · WDM – compatible video capture device	1
PC - CLIENT:	· Microsoft® Windows® 2000 Professional (Service Pack 3 or higher) or Microsoft® Windows® XP Professional (SP 1a) · 1000 MHz Pentium 4 Processor · 256 MB RAM · 10 GB HDD · CD-ROM Drive · 2 RS-232C Ports · 16-bit SoundBlaster (or compatible) audio adapter · WDM – compatible video capture device	
	Network configuration: workgroup or domain (more secure).	0
Monitor	19I flat screen	1
Key & M	Wireless Keyboard & Mouse	1
Speakers		1
Cables	Single RSA plug to UPS & 2 X kettle plugs	3
UPS	15 Min standby	1
Camera	Colour high resolution	1
Lens	12mm	1
Power supply	12V	1
Cables	RJ 179	1
Connector	BNC to RCS connector	1
MAGLOCK	For single door / turnstile	1
Card reader	KeyMaster AC-1300 is a proximity reader with12-key PIN pad.	1
	Cards	500
	The Wiegand-26 Non-keypad Reader (Metal Housing) Impro code IWM904-1-0-GB-XX.	0

Appendix II– FACE VERIFICATION LINKED TO ACCESS CARD SOFTWARE MANUAL

CONTENTS PAGE

SYSTEM REQUIREMENTS

The software is compatible with Windows 2000 and XP. The minimum system configuration requires a Sound Blaster compatible sound card and a video capture card compatible with DirectX 8.0, in addition to the standard PC hardware. Minimum hardware requirements are listed below:

512 M Byte RAM
4.200 GHz Pentium Processor
5 G Byte HD
CD ROM
2 COM ports / 2 USB ports
Audio card compatible with 16 bit SoundBlaster
Video capture card or USB video converter compatible with WDM (DirectX 8.0)

The Veraport system requires a Wiegand to Serial Interface circuit board and a Digital I/O with relay circuit board which I have mentioned in the previous email.
Both devices are as follows:

- **Stand alone circuit boards**
- **Not PC bus devices, i.e. Not PCI, Not ISA, Not AGP**
- **Roughly 100 mm square**
- **Require 12 VDC power from some external supply**
- **Communicate to the host PC via RS 232 Serial port (Host PC must have 2 serial ports or some adaptor which can facilitate this.*)**
- **Employ unique communications protocol**
- **Use terminal blocks for *most* electrical connections. (Digital I/O is done directly off of circuit board traces and pads.)**

SERVER:

· Microsoft® Windows® 2000 Professional (Service Pack 3 or higher) or Microsoft® Windows® XP Professional (SP 1a)

· 1.6 GHz Pentium 4 Processor

· 512 MB RAM

· 40 GB HDD

· CD-ROM Drive

· 2 RS-232C Ports

· 16-bit SoundBlaster (or compatible) audio adapter

· WDM – compatible video capture device

CLIENT:

· Microsoft® Windows® 2000 Professional (Service Pack 3 or higher) or Microsoft® Windows® XP Professional (SP 1a)

· 1000 MHz Pentium 4 Processor

· 256 MB RAM

· 10 GB HDD

· CD-ROM Drive

· 2 RS-232C Ports

· 16-bit SoundBlaster (or compatible) audio adapter

· WDM – compatible video capture device

Network configuration: workgroup or domain (more secure).

DEMONSTRATION PROGRAM

This illustrates the functionality of LODGE facial recognition technology in a variety of practical applications. These being:

i) Facial recognition in classification mode (one-to-many identification)
ii) Facial recognition in verification mode (one-to-one identification)
iii) Facial verification combined with proximity card
iv) Facial verification combined with finger print recognition (dual biometric)
v) Facial verification combined with finger print recognition and proximity card.
vi) Operation of R410/R810 relay controller (i.e. for opening door, controlling signs, etc.)

In addition to the above, the user has the ability to modify text strings that permit customization of computer-generated speech when the system is operating in classification mode.

INSTALLATION

To install the LODGE Discovery System insert the LODGE installation CD into the CD ROM drive. The installation will proceed automatically, or click on "setup.exe" in the main CD directory. Prior to installation, please uninstall any previous versions of LODGE facial recognition programs. For first time installs a series of standard installation screens will appear requiring input of user name, environment setting, and installation target directory. Following this the screen (shown below) will appear.

By default the following components are installed:

i) LODGE facial recognition demonstration program
ii) LODGE facial recognition OCX control for stand-alone applications
iii) Visual Basic sample programs
iv) Documentation/Help files
v) Video capture driver for Belkin USB VideoBus II
vi) Extensions for optional speech synthesis and overlay text displays
vii) Controller extension for R810/R410 relay card
viii) PerfectMatch Fingerprint Reader
ix) PcProx proximity card reader

This LODGE face recognition program contains soft lock protection. Following the initial installation you will encounter the following screen when running the demonstration program or using the OCX control. Please follow the instructions indicated on this screen BUT E-Mail the code to images@I-Cube.co.za. Once the NDA and license agreement have been signed and received, your code will be e-mailed back to you.

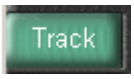
The locking code returned to you must be entered into the text box located at the bottom of the screen.

NORMAL OPERATION

Select the FRS Demo from the desktop or from the start menue.

The main screen of the LODGE face recognition demonstration program is shown below. The control pushbuttons on the left side of the screen allow the user to run the program in the various modes (i.e. track only, classify, verify) as well as adjust operational settings.

Functions provided by the control pushbuttons are described below:



Enables facial tracking. Both the demonstration program and OCX control are able to track up to four faces simultaneously. Classify and Verify operations must be enabled separately by clicking on pushbuttons located below "Track".

Enables the classify operation (one-to-many identification). If tracking is not currently enabled, operation of this pushbutton will enable both "Track" and "Classify". Both the demonstration program and OCX control are able to perform classification in real time, with up to several hundred people enrolled within the data

base. If the voice greeting extension has been installed, the program will speak the individuals name followed by a randomly selected phrase.

Enables the Verify operation (one-to-one identification). If tracking is not currently enabled, operation of this pushbutton will enable both "Track" and "Verify". Verification requires input of the users ID number. Both the demonstration program and OCX control are able to verify from a database of several thousand people. If the voice greeting extension has been installed the program will speak the individuals name followed by a randomly selected phrase.

Extensions have been provided which combine the verify operation with a proximity card reader (pcProx), finger print verification (PerfectMatch) and a D/O controller for door operation (810/410 relay controller). In the event that the pcProx extension has been loaded, the verify operation is initiated automatically when the user activates the proximity card. In the event that the PerfectMatch fingerprint extension has been loaded, the system will request that the user place their finger on the fingerprint reader for additional verification (dual biometric). In the event that the digital output (D/O) extension is installed and activated, the D/O controller closes the relay contact for N seconds following a successful verify or classify operation.

This pushbutton starts the enrolment process for an existing or new user. The following form is shown when this pushbutton is activated.

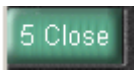
The user must type in their first and last name. Entering a user ID number is optional. In the event that the pcProx card extension is installed this number corresponds to the card ID number. In addition, an ID number must be entered in order for the verify operation to work. Once data has been entered click on the OK pushbutton and the system performs the enrolment procedure.

During enrolment a series of vocal commands are issued instructing the subject to look left and right. Only one person should be in view of the camera during enrolment. An individual may be enrolled more than once (this increases the number of images used in training and increases recognition accuracy), however take care to ensure the same name is entered on each enrolment. During one enrolment procedure the system will capture 100 images (default) and place these in the facial database. These images are used to train a neural assembly to differentiate between the enrolled user and other individuals.

Following capture of the facial images, the following screen will be displayed providing the option to delete images from the collection.

Images are removed by clicking on an image which highlights the selected image using a red boarder, and then clicking on the "Remove Image" pushbutton.

This allows the user to modify the default settings used in the facial recognition program. The options screen is shown below and described in the following section..



The normal display shown on the right side of the video area is a picture clip of the identified individual. When this pushbutton is enabled the system will display the pictures and names of the five closest matches, along with the associated recognition confidence values. The range of the confidence value is from -1 (low recognition confidence) to +1 (high recognition confidence).

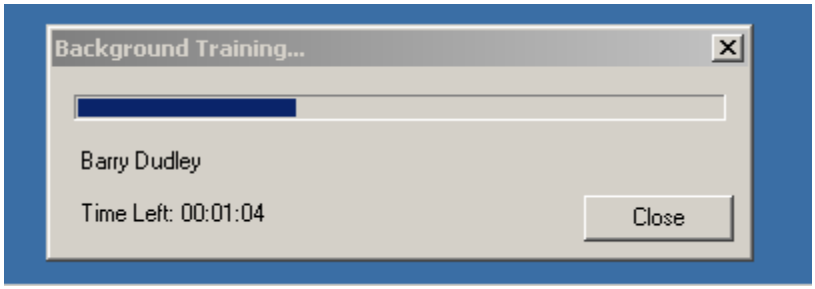
This enables full screen mode for the video display. All other controls normally shown in the default display mode will become hidden. The full screen display mode is shown below:

The pushbutton controls may be displayed while in full screen mode by moving the mouse to the top left side of the display screen.

Terminates the program.

DATABASE

The "Database" menu allows the user to edit the facial database, as well as add or remove individuals from the active list of users. Selecting the 'Edit Database' menu item will bring up the screen shown below. The 'Clear & Retrain All' menu item clears cortical memory for the classification assemblies (i.e. clears the face recognition templates) and initiates the "New Registrant" training procedure over all users enrolled within the system. The "Show Training Status" menu item displays the name and training progress for the continuous training operation.



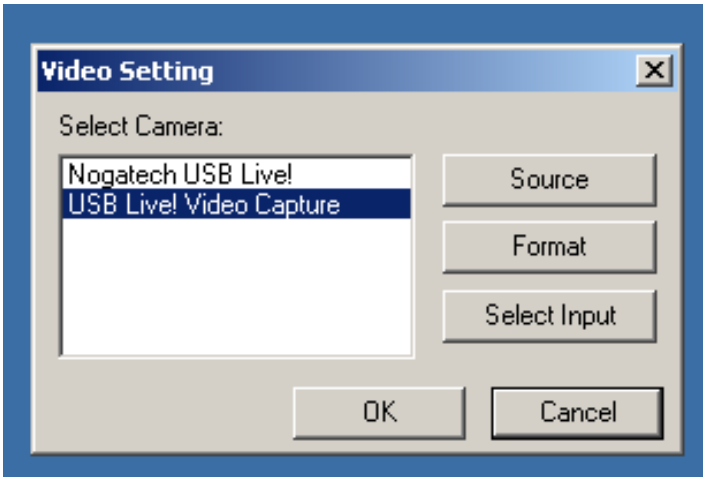
This above "Edit Database" screen allows one to add or delete individuals from the active list. Adding an individual to the active list is performed by enabling the check box located to the left of the name. The user names are listed in the selection box located on the lower left side of the form. Specific images recorded for an individual user may be removed by clicking on the image located at the right side of the form, and subsequently clicking the 'Remove Image' pushbutton located at the lower left. Removing an individual from the database is performed by highlighting the name in the main list box and clicking on the 'Remove Person' pushbutton.

User data located in the "Personal Information" panel may be edited by entering new values within the associated text boxes and clicking the "Update" pushbutton.

FACE RECOGNITION OPTIONS

The "View" menu allows the user to modify various display options for the program, and change video settings. The ‘Zoom’ menu item allows one to adjust the size of the video display area. The "Show Masks" menu item allows the user to display the various masks, eliminating from tracking regions of low variance, low movement and non-skin color from the tracking region.

‘Classify Status Bars’ changes the visible status of the display bar located at the bottom of the main screen associated with classification. The ‘Tracking Status Bars’ changes the visible status of the display located at the lower left of the main screen associated with tracking “knowbots”. Up to four knowbots may be placed on each image frame and the status bars display the detection level for facial images. The final menu item allows one to adjust the video capture settings. Operation of this menu item will bring up the following screen.



The installed video drivers are shown in the list box. The appropriate driver is selected by clicking on the driver label and clicking OK. Pushbuttons "Source" and "Format" bring up the appropriate driver settings form, and "Select Input" is used by certain drivers for selecting either S-video or Composite input.

LOGGING UNTILITY

The LODGE Discovery System includes a basic logging utility for recording statistics on the various activities performed by the system. Recording of the activity log is enabled or disabled through the Options form as described in the previous section. The log entries may be viewed or printed to text file using the LogView.exe program located on the main directory of the LODGE FRS Discovery System. The activity log viewer program is shown below:

The following four categories of activities are logged by the face recognition program:

- **Enrollment**
- **Classify**
- **Verify Success**
- **Verify Failure**

Statistics that are recorded along with the activity type are:

- **Computer Name**
- **Time**
- **Date**
- **User ID Number**
- **User Name**
- **Head Position (X, Y, Size)**
- **Facial Image**

The above statistics are displayed in the log viewer, captured images are referenced by file name. The user may view the captured image by doubled clicking on the corresponding row, or selecting the "View Image" button on the toolbar.

Bibliography

Available on request

References

Available on request

The opinions expressed in this document are the views of the authors and do not necessarily reflect those of the views of I-Cube, any site, or any other party.

THE END