

**Proposal for  
PORT**

for

# **ADVANCED VEHICLE ACCESS CONTROL SOLUTIONS**

## **Incorporating LICENSE PLATE RECOGNITION, DIGITAL RECORDING and Biometric Facial Identification / VERIFICATION SOLUTIONS**

*Compiled / Supplied by*

Dawa Sewbalak

***Power Automation***

**E-Mail: [power.auto@intnet.mu](mailto:power.auto@intnet.mu)**



Sunday, 29 May 2005

*In conjunction with I-Cube*



## TABLE OF CONTENTS

1	Confidentiality Clause .....	4
2	Declaration.....	5
3	Acknowledgements.....	6
4	Abstract.....	7
5	Description of Requirement.....	12
6	Issues for Consideration .....	13
7	Solution Proposed.....	14
7.1	Solution Design.....	14
7.1.1	Vehicular Traffic .....	14
7.2	Face Recognition System Description.....	16
8	<b>FACIAL VERIFICATION Equipment Requirement .....</b>	<b>18</b>
8.1	HARDWARE.....	18
8.2	Additional Items .....	19
16	<b>Explanation of Biometrics.....</b>	<b>20</b>
8.3	Normal process from here .....	21
9	<b>EQUIPMENT Considerations .....</b>	<b>22</b>
	Conditions .....	25
9.1	Acceptance .....	25
9.2	Standard Terms and Conditions.....	25
10	<b>Rental Option.....</b>	<b>26</b>
10.1	BENEFITS OF POWER AUTOMATION RENTAL.....	26
11	<b>Conclusion.....</b>	<b>27</b>
12	<b>Introduction - Role Players.....</b>	<b>29</b>
12.1	Introduction.....	29
12.2	Marketing.....	29
12.3	Security.....	29
12.4	Operations .....	30
12.5	Legislative.....	30
13	<b>LPR Scope Of Work.....</b>	<b>31</b>
13.1	Full description of system topology offered .....	31
13.2	Sample sequence of operation.....	33
13.3	Suggested LPR Procedure: .....	35
13.4	Schedule Of Equipment Specifications .....	36
14	<b>LPR Equipment Quote .....</b>	<b>37</b>
15	<b>Software Quote.....</b>	<b>40</b>
15.1	FACE RECOGNITION SYSTEMS .....	42
16	<b>Privacy discussion .....</b>	<b>44</b>
17	<b>LICENSE PLATE RECOGNITION LINKED TO FACIAL VERIFICATION USER MANUAL .....</b>	<b>46</b>
18	<b>Installation Quote .....</b>	<b>56</b>
19	<b>Equipment Requirement .....</b>	<b>57</b>
20	<b>Digital Recorder Integration .....</b>	<b>58</b>
21	<b>FACIAL IDENTIFICATION SOFTWARE USER MANUAL.....</b>	<b>59</b>
21.1	How to use I-CUBE Facial Search .....	59
21.1.1	Enroll.....	59

21.1.2	Batch Enroll.....	59
21.1.3	Search.....	61
21.1.4	Browse Database.....	61
<b>22</b>	<b>FACIAL VERIFICATION SOFTWARE USER MANUAL.....</b>	<b>63</b>
22.1	Basic Operation .....	63
22.1.1	Connecting to Server.....	63
22.1.2	Standard View.....	64
22.1.3	Full Screen View .....	68
22.2	Setting Operating Parameters.....	69
22.2.1	General Tab .....	69
22.2.2	Enrollment Tab.....	70
22.2.3	Tracking Tab .....	71
22.2.4	Classify Tab .....	73
22.2.5	Verify Tab.....	74
22.2.6	Image Filter Tab .....	75
22.2.7	Extensions .....	76
	Training .....	80
22.3	Server Database.....	81
22.3.1	Editing the Database .....	81
22.3.2	Exporting Users.....	82
22.3.3	Importing Users.....	82
22.3.4	Regenerating Templates .....	83
22.3.5	Pre-Registration of Users .....	83
22.4	Enrolling from Static Images .....	84
22.5	Activity Log Viewer.....	86
22.5.1	Showing the Activity Log .....	87
22.5.2	Filtering an Existing View .....	87
22.5.3	Opening a New View.....	87
22.5.4	Saving the Activity Log .....	87
22.5.5	Loading the Activity Log .....	88
22.6	Modifying Control Button Configuration.....	88
22.7	Setting Up Speech.....	88
22.8	Video Settings.....	89
22.9	FRS Server Manager .....	89
22.9.1	Shutting Down the FRS Central Server .....	90
22.9.2	Restarting the FRS Central Server .....	90
22.9.3	Viewing Connected Client Computers .....	90
22.9.4	Managing FRS Training Servers .....	90
22.9.5	Selecting the FRS Database .....	91
22.10	FRS Training Server Manager.....	91
<b>23</b>	<b>Biometric Intelligence Overview .....</b>	<b>93</b>
23.1	HNeT Tools.....	93
23.2	Performance Features .....	93
23.3	General Comparisons .....	94
23.4	The Monte Carlo Test .....	94
23.5	Comparison 1 – Learning 100 Stimulus-Response Patterns .....	95
23.6	Comparison 2 – Learning 500 Stimulus-Response Patterns .....	95
23.7	The Biology.....	95
<b>24</b>	<b>Definitions .....</b>	<b>97</b>
<b>25</b>	<b>Special Terms and Conditions .....</b>	<b>100</b>
<b>26</b>	<b>INDEMNITY .....</b>	<b>103</b>

# 1 Confidentiality Clause

Sunday, 29 May 2005

Due to the strategic importance of this work it would be appreciated if the contents remain confidential and not be circulated for a period of two (2) years.

Sincerely

Signed.....

Date.....Sunday, 29 May 2005

Dawa Sewbalak

**Power Automation**

E-Mail:power.auto@intnet.mu



## 2 Declaration

This research is done specifically for:

### PORT ACCESS CONTROL CLIENT

Date: Sunday, 29 May 2005

The opinions expressed in this document are the views of the authors alone and do not necessarily reflect those of the views of DECALINK LTDA., management, employees, or any other party. Numerous assumptions have been made and many of these would have to be validated at the commencement of the project.

Signed.....

Date.....Sunday, 29 May 2005

Dawa Sewbalak

*Power Automation*

E-Mail:power.auto@intnet.mu



### 3 Acknowledgements

We would like to thank the following for assistance:

Barry T. DUDLEY I-CUBE (I3 - Integrated, Intelligent, Imaging)  
(MBA {IT}; MSc {Image Analysis}; BSc {Brewing}; BSc Hons {Waste Technology})

LICENSE PLATE RECOGNITION AND FACIAL IDENTIFICATION SOLUTIONS

<http://www.i-cube.co.za>

Cell: +27 (0) 82 562 8225

MADADENI

PH +27 (0) 31 764-3077

82 Kloof Falls Rd

Fax 031-7643077

Kloof, Durban, Kwa-Zulu Natal, 3610, South Africa E-mail: [info@I-Cube.co.za](mailto:info@I-Cube.co.za)



## 4 Abstract

An PORT ACCESS CONTROL engages in a constant battle to use technology to enhance their competitive position and detect and prevent crime. In order to overcome the problems associated with being at this technological edge, **Power Automation** selects rock solid technology and integrates and supports the technology. Implementing the enclosed solutions will allow all role players to gain a competitive advantage in terms of marketing, customer relations, security and surveillance.

In order to overcome the problems associated with entry and exit operations where management cannot be present, the possession of accurate information regarding what occurs, as well as a way to quickly and accurately obtain that information, is crucial. **Power Automation** will supply and install the latest digital video technology that will provide a tool that will dramatically change current operations for the better.

The proposed solution consists of cameras connected to a digital recorder, which will allow both real time and recorded view of the entry and exit lanes. The entry area in particular will be monitored, linking all number plates, vehicles and driver seen to the database and video footage. The residence plates will trigger the facial verification, which if the person matches the facial template in the database, will allow the boom to open on entry and departure.

Visitors and cars pre-registered will have the ability to automatically gain entry. The software will allow the guard to manually enter the number of people in a visitor vehicle plus link any existing card based access control system to visitor cars, if required. On exit the guard will then be prompted to confirm that the same number of people exit as came in. The on site digital recorder which will act as a base station from which recorded images from all the cameras can be reviewed from remote locations.

With the POWER AUTOMATION systems Facial Identification software all visitors are logged, allowing any suspicious person to be immediately searched against the "suspects" database, and the homeowner's database or the "known workers" database, immediately identifying the person.

**CLIENT**

**Sunday, 29 May 2005**

**ADDRESS**

**Att: Mr. CLIENT**

**TITLE**



Dear **CLIENT**

## **PORT ACCESS CONTROL – DIGITAL VIDEO MANAGEMENT SYSTEM PROPOSAL**

Thank you for affording **Decalink Ltda** the opportunity to quote on the installation of a digital video management system at the ESTATE, including the use of a Vehicle Number Plate Recognition System as detailed herein.

"As leading specialists in integrated intelligent imaging, we propose the attached solution which, if implemented correctly, has the potential to solve your customers problems, enhance some of your existing security services, unlock additional potential and, hopefully exceed your expectations.

The License Plate Recognition linked to facial capture and verification solution allows: -

- Image trigger via a loop on the road;
- Multiple image capture by a high resolution black and white camera;
- License plate finding within the image;
- License plate number reading at an accuracy over 99.95% (with multiple cameras used in stereo);
- Linking of the license plate with car colour and shape (if required);
- Linking of license plate number with a name and display of this information on ELECTRONIC DISPLAY (if present) when the vehicle is detected;
- Linking of license plate number with a facial template allowing facial verification and automatic updating of the template as the person ages / changes;
- Log of number and image of all vehicles and driver who enter and exit the facility;
- ◆ Image capture of the person from a high resolution colour camera;
- ◆ Face finding within the image;
- ◆ Searching central database and display of results;



- ◆ Entry of all images and details that are not in the database Linking of the face with various fields (such as ID no., name, Birth, Sex, Eye, hair Colour, Ht, Wt, Address, City, State, Zip, Country) for entry into the suspicious persons database;

As leading specialists in using visual technology to solve customer problems and increase profitability we propose the attached solution.

This solution allows management to BE EVERY WHERE AT ONCE and focus on

- ✓ Productivity improvement,
- ✓ Loss control,
- ✓ Vehicle monitoring,
- ✓ Safety management,
- ✓ Ensures that staff and managers spend time where they are needed most.

This Digital Management Solution will be implemented into your business to help you better manage your business and in the long run improve your profits through increased productivity levels and better work practices.

With POWER AUTOMATION Digital Management Solutions you will have better control over access control, visitors, deliveries, contractors and staff.



Implementing our digital system throughout your premises will give you a visual audit trail of cars, giving you much more material to work with when making managerial decisions.

The system doubles as a security and Visual Management System, and since it's an "open architecture system," other compatible systems can be incorporated into your system.

POWER AUTOMATION specialises in integrated digital CCTV Management Systems that are designed according to each client's unique requirements and specifications. Intelligent digital CCTV management systems by POWER AUTOMATION presents operators only with the information that they need to re-act upon and provides management with instant retrieval of vital recorded footage. The POWER AUTOMATION option is not simply a security system, it allows management to focus on productivity improvement, loss control, safety management, procedure audits, equipment maintenance, time and motion studies and ensures that managers and security staff spend time where they are needed most in their operational functions.

In the rapidly changing digital world it is important to understand that information and the rapid and efficient interpretation of this information is the key to effective decision-making.

POWER AUTOMATION provides the artificial intelligence on a digital platform to turn "Images to Intelligence". Customised application specific algorithms provide real-time processing; detection, storage and rules based decision support systems of pre-configured events, with the added advantage of being able to artificially interrogate the recorded database. In

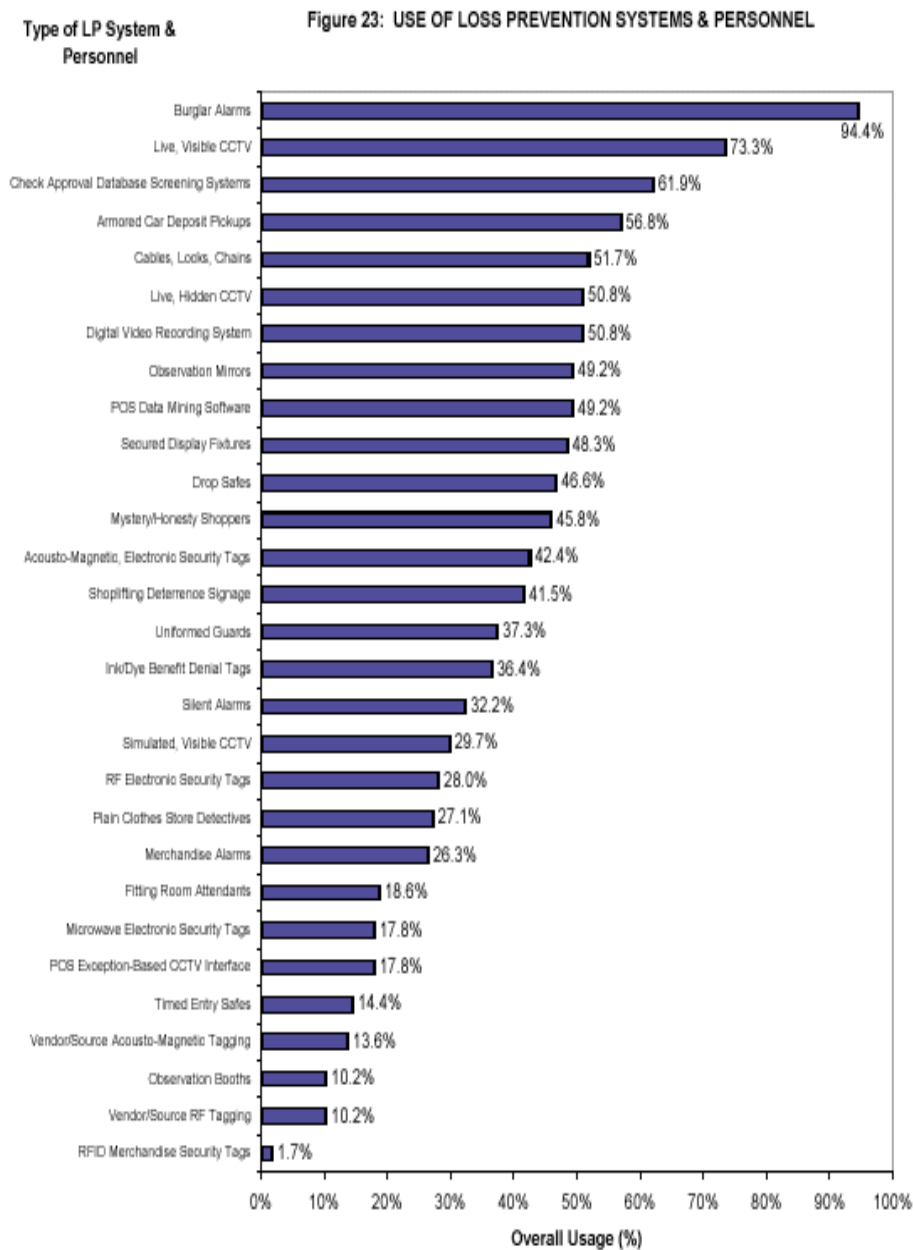


Figure 1 Use of CCTV systems is on the increase

essence these systems automate security, process and inspections within an operation, reducing manpower and the inherent human failure.

A 12-month guarantee is applicable in respect of all equipment installed and workmanship. A separate maintenance contract can be negotiated for the balance of the rental period after the expiration of the guarantee period. The system requires either 12V or 220-volt plug points and sufficient light for the cameras, although the cameras quoted on have a low light specification. All training to the relative users of the system to the point of competency is provided at no additional cost.

Thanking you in anticipation of the quotation being accepted and your instructions to proceed with the compilation of the rental documents and thereafter installation of the system. Please be assured of my best attention at all times.

Dawa Sewbalak

**Power Automation**

E-Mail:power.auto@intnet.mu



## 5 Description of Requirement

The requirement, as stated, is for access control to an PORT ACCESS CONTROL with MULTIPLE (X) gates.

Each gate is assumed to have one lane IN and one gate OUT (possibly separate lanes, I.E. 1 lane IN, 1 lane OUT, or same lane, bi-directional):

- Where two types of vehicles/drivers are present (those in the database (enrolled) and those NOT present in the database (visitors);
- Where both license plate and driver face are enrolled in the database access will be allowed based on verification of the driver's face with the license plate on ENTRY & EXIT;
- Where NOT PRESENT in the database access MONITORING of driver face and license plate will occur on ENTRY & EXIT
- Allowing matching of license plate with original drivers face on exit
- Each gate will be able to handle a vehicle every 3 seconds per lane;
- Each gate will be able to manage over 750 000 users in the database, plus an unlimited number of vehicles which are not in the database;
- The GUI will report if:
  - The vehicle is not registered;
  - In the database but not allowed access;
  - In the BLACK LIST
  - Vehicle and driver match (allowing boom to open)
- The GUI will allow each vehicle to be granted access based on gate number; driver and various other criteria as required (please specify);
- Reports are detailed and comprehensive, including:
  - Counts;
  - Vehicle registration no's
  - Gate history
  - Date history
  - Vehicles in the database, visitors and other categories
  - Watch list
  - Etc.
- The 2<sup>nd</sup> means of identification can be colour, shape, size, card or fingerprint.
- Integration to parking ticket systems can be provided
- All technical specifications are exceeded and detailed below.



The requirement is to provide Licence Plate Recognition (LPR) technology linked with FACIAL VERIFICATION to facilitate ACCESS CONTROL of allowed vehicles and associated drivers entering and exiting the EDUCATIONAL FACILITY.

## 6 Issues for Consideration

There are a few points that should be borne in mind during the compilation, review and assessment of this proposal and the subsequent manner in which this will progress should your decision be favourable to move forward:

- This proposal outlines what can be done in order to address the stated requirements and does not delve into too much detail. (Although much of the detail is supplied in the Appendix.) The detail regarding the actual implementation process is not addressed, but is estimated in the Financial Considerations section.
- Our philosophy for solution crafting highlights the fact that all solutions consist of 4 primary elements: people, process, technology and information. The technology aspect is addressed in this proposal. The other aspects are normally addressed in the project scoping workshop which will typically commence once there is agreement to proceed.
- The success of implementations of this nature is dependent on a formalised project approach where expectations and deliverables are clearly expressed, recorded and agreed. Ensuring open dialogue prior to implementation allows for all parties to ensure that all parties agree. Scope management is also crucial to ensure proper implementation. We all know what assumptions do and are!
- A medium level project schedule with project report will be supplied after the project kick-off session.
- There is existing equipment that may be used in this solution offering, but we have not considered this at this time. This will be reviewed at the kick-off session where all the existing cable and equipment will be assessed and integrated where possible.
- There may well be some information that has been omitted as a detailed site inspection has not yet been conducted.
- There are direct benefits to security, legal matters relating to security breaches, operations, as well as an additional marketing tool to enhance value to owners.



## 7 Solution Proposed

The proposed solution would enhance the image of the PORT ACCESS CONTROL and would also provide huge practical security access control enhancements to the day-to-day operation. The offering to address the stated requirements will be tackled as a complete entity but can be phased or broken down into its components and implemented as separate items, if required. Some technical terms will be used and a glossary of terms is supplied as an Appendix to this document to assist with understanding (should it be required.)

### 7.1 Solution Design

A basic matter of understanding the difference between Identification and Verification is crucial for the development of appropriate solutions.

- **Identification** is the assessing of the car or object presented for identification and attempting to derive a match from the repository of information (typically a database). This process requires a search through a database and the search can be sequential or can be built on certain criteria to ensure more effective lookup. It is a one-to-many review.
- **Verification** is the process whereby an item for identification is presented, either a license plate, PIN, proximity card or ID card, and an additional criteria (in this case facial) is used to validate that the car presenting the item is actually who they are claiming to be. This is a one-to-one review.

Each of these options are possible with the technology proposed, but each requires a different approach to the actual implementation and the associated processes.

#### 7.1.1 Vehicular Traffic

This specific system will allow for the capturing and analysis of images of licence plates, front and rear (which would also cater for trailers) to ensure an accurate record of vehicles entering and exiting the EDUCATIONAL FACILITY. Each vehicle could be classified as employee, owner, visitor, contractor, supplier, etc. Rules for access could be defined for each vehicle and access could be granted accordingly.

The system proposed would analyse the licence plate and the colour and shape of the vehicle for the match and would then operate the boom. If there is a discrepancy, then the security personnel will be alerted and appropriate intervention will then take place.



When visitors are scheduled to arrive, security can be contacted to enter the registration of the vehicle into the system and when the car arrives access is allowed and a welcome message displayed on the visual display (if supplied). Access for visitors can be defined for the period that they will be there and, while the record will still in the DB, it will be in a status that would recognize but not allow access.

Facial recognition could be added to this to further enhance the security access control system to log all drivers with the vehicles. Facial verification would ensure that there is a match between vehicle and designated driver. It will be possible to link multiple drivers to multiple vehicles so the system would not be restrictive from that perspective.

The idea is to remove much of the responsibility of assessing vehicles entering to dealing with the anomalies and allow normal authorized vehicles to proceed without delay.

**COMPONENTS**



The main system would be installed on a server controlling the process. This would house the database as well as the application that handles the analysis. It would be linked to a trigger mechanism (either a loop at the entrance or the presentation of the proximity tag), the boom and the various cameras.

**OPERATIONAL ISSUES**

All PORT ACCESS CONTROL personnel, owner and employee vehicles would initially need to be registered on the system and an appropriate mechanism for doing this would have to be agreed with the PORT ACCESS CONTROL and the various stakeholders.

Contractor and supplier vehicles would also need to be registered through a similar process and rules governing their access rights would need to be agreed.

Processes for visitors and ad-hoc entrance would also be agreed and would need to be implemented.

**In Summary ...**

The License Plate Recognition and facial capture solution allows: -

- Image trigger via a loop on the road;
- Multiple image capture by a high resolution cameras in STEREO (front and back);
- License plate finding within the image;
- License plate number reading at an accuracy over 99.95% (with multiple cameras used in stereo);
- Linking of the license plate with a drivers facial template AND / OR an IMPRO access card (if enhanced security is desired);
- Linking of the license plate with car colour and shape (if required);
- Linking of license plate number with a name and display of this information on ELECTRONIC DISPLAY (if present) when the vehicle is detected;
- Log of number and image of all vehicles and driver who enter and exit the facility;
- Facial capture and identification on exit (if requested);
- ◆ Image capture of the person from a high resolution colour camera;
- ◆ Face finding within the image;
- ◆ Searching central database and display of results;
- ◆ Entry of all images and details that are not in the database Linking of the face with various fields (such as ID no., name, Birth, Sex, Eye, hair Colour, Ht, Wt, Address, City, State, Zip, Country);
- ◆ Facial verification based on license plate or access card.



## 7.2 Face Recognition System Description

The Face Recognition System is used to assist in identification.

The surveillance operator manually compares the live or recorded images and the saved facial images against a database of previously saved face images, with an operator reviewing the results and making the decision. This means that the accuracy of the system is NO LONGER crucial, as the system presents information to a human operator to make the final decision. One is using the face recognition system to check if the person has been seen before, with the operator looking at the results to check the match. This is due to the fact that the following affect the results of ANY face recognition system: Lighting, quality of original image in the database, temporal affects (time and ageing), glasses, hats, shadows, hair style or lack of hair, background, size of face in the image, and a WIDE RANGE of other environmental conditions. One is using face recognition to assist in IDENTIFICATION of repeat trouble makers, illegal entry, shop lifters, bad check passes and then the operator decides on the appropriate action to follow.





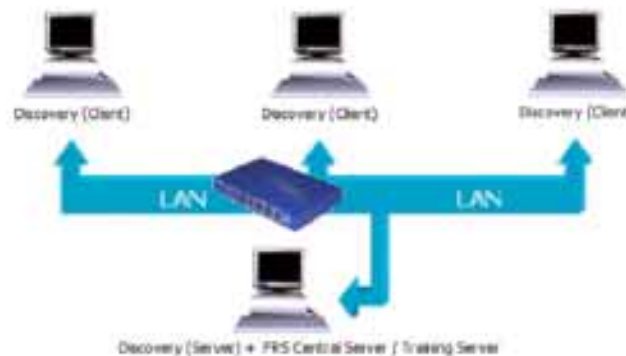
ITEM	DETAIL	No. Provided
Face Recognition software	Includes ability to add facial images and personal details, create multiple Databases	1
	Ability to capture from a VIDEO FOR WINDOWS source and view closest matches, for full details see the user manual below	1
Frame Grabber	Video capture device	1
PC	<ul style="list-style-type: none"> <li>• Microsoft® Windows® 2000 Professional (Service Pack 3 or higher)</li> <li>• 1000 MHz Pentium 4 Processor</li> <li>• 128 MB RAM</li> <li>• 10 GB HDD</li> </ul>	If required
Monitor	19" flat screen	If required
Key & M	Wireless Keyboard & Mouse	If required
Cables	BNC to RCA cable	If required
UPS	15 Min standby	If required

**TRAINING**

1 Day ON SITE training (limited to 6 people)

**MAINTENANCE**

MAINTENANCE (ongoing support, FREE software updates,):



The I-CUBE Facial Identification system is based upon a two-tier Client/Server architecture. The system consists of a single Server application connected to multiple Client applications. All data pertaining to images, associated text and biometric templates are stored centrally on the I-CUBE Facial Identification Server and facial recognition operations may be performed on either Server or Client machines. The I-CUBE Facial Identification System can store an unlimited number of individuals for use in identification operations.

The system is set-up such that the Server machine contains the Central Server, FRS Training Server, FRS Database and Client application running locally. These components provide the core biometric template generation, data storage and communication to external Client applications. For a more in-depth description of please request the appendix.

## 8 FACIAL VERIFICATION Equipment Requirement

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

### I-CUBE FACIAL VERIFICATION Client

Microsoft® Windows® 2000 Professional (Service Pack 4) or Microsoft® Windows® XP Professional

- 3 GHz Pentium 4 Processor
- 1 GB RAM
- 1 TB HDD
- CD-ROM Drive
- WDM – compatible video capture device

### I-CUBE FACIAL VERIFICATION Server

- Microsoft® Windows® 2000 Professional (Service Pack 4) or Microsoft® Windows® XP Professional
- 3 GHz Pentium 4 Processor
- 1 GB RAM
- 1 TB HDD
- CD-ROM Drive
- WDM – compatible video capture device



The performance of the I-CUBE FACIAL VERIFICATION CLIENT PC is subject to at least an ISDN connection to the central server.

The I-CUBE FACIAL VERIFICATION requires a skilled operator who has either been trained or has read and understood the I-CUBE FACIAL VERIFICATION user manual.

### 8.1 HARDWARE

A good facial image is required, obtained from a camera optimally positioned for the driver facial capture

The S-912 **USB Video Grabber** with Stereo Audio is the ultimate USB video connector featuring built-in video and audio ports. Its RCA and S-Video ports allow you to easily import video from CCTV cameras, TV's, VCR's, camcorders, or any other analogue devices. The audio port supports stereo audio recording.

**Specifications:**

<b>Model</b>	<b>S-912</b>
<b>PC Interface</b>	USB Rev. 1.1
<b>Supports camcorders, TV, VCR, video game player, analogue cameras, etc.</b>	
<b>Video Standard</b>	NTSC, PAL, SECAM
<b>Signal Input</b>	Composite (analogue) or S-Video
<b>Audio Input</b>	Stereo Audio
<b>Capture Rate</b>	25 fps at CIF (320x240), 10-15 fps at VGA (640x480)
<b>Frame Size</b>	QCIF (160x120) to VGA (640x480)
<b>Hardware Compression</b>	Yes
<b>Software Interface</b>	Video for Windows, TWAIN interface, WDM driver
<b>File Formats Supported</b>	BMP, AVI, PCX, TIF, JPG, TAG
<b>Data Format</b>	YUV 4-2-2, YUV 4-2-0, RGB
<b>O/S Support</b>	Microsoft Windows 98, 98 SE, 2000, ME, XP, Mac OS 8.6, 9.0
<b>Power</b>	Provided by USB port
<b>Operating Temperature</b>	0 C to 50 C degrees (Non-Condensing)
<b>Storage Temperature</b>	-10 C to 60 C degrees (Non-Condensing)

**Minimum System Requirements:**

- Intel Pentium II 350 MHz CPU or above
- 1 Free USB Port
- 512 MB of RAM
- Microsoft Windows 2000, XP,

\* All specifications are subject to change without notice

\* All brand names and trademarks are the property of their respective owners

**8.2 Additional Items**

All events will be captured on a digital video recorder to allow access to real time and historical records.

## 16 Explanation of Biometrics

In order to work with the POWER AUTOMATION Facial VERIFICATION system, it is beneficial to understand the basic concepts of system operation.

Each User that is registered within the POWER AUTOMATION Facial VERIFICATION system has an associated facial biometric template, which contains the information (based on enrollment images) used to identify the User.

Biometric access control relies on three mechanisms: enrollment of the users biometric data (facial images), generation of the biometric templates using the enrolled facial images, and subsequent VERIFICATION of the user, applying the biometric template.

### Tracking

In order to make face VERIFICATION non-intrusive and flexible, the POWER AUTOMATION Facial VERIFICATION system automatically locates and follows any human face that is within the camera's field of view. This allows the individual to act in a natural manner with freedom of movement and locomotion, and minimal cooperation with the system.

### Enrolment

Enrollment is the capturing and storing of facial images of the user, in order to generate the facial biometric template. The greater the volume and quality of the enrollment images, the faster and more reliably the system will recognize the user during subsequent verify or classify operations. Enrollment is performed by clicking the Enroll button on the control bar of the POWER AUTOMATION Facial VERIFICATION main window.

### User Registration

Within the POWER AUTOMATION Facial VERIFICATION system, a user may be registered before they are enrolled. This means that users may be entered into the POWER AUTOMATION Facial VERIFICATION database without enrollment of facial images or storage of an associated biometric template. Registration may be performed for one user at a time through a dialog, or for many users using an ASCII text file. Registered users are automatically enrolled the first time they present their ID token (i.e. proximity card, keypad) through a Wiegand device, or enter their user ID manually through the Enroll control button.

### Template Generation

Biometric templates are generated and continuously updated through a process referred to as "Training"; using the facial images captured during the enrollment operation. Further enrollment (i.e. capture of additional facial images) may be performed during subsequent verify operations. This ensures that the biometric templates are as up-to-date as possible.

### **8.3 Normal process from here ...**

The standard process after due consideration and finalization of various components is to formalize the agreement to move forward with an order to commence the project. This would take the form of either signed acknowledgement of acceptance of the proposal, a letter indicating acceptance or a formal order number.

Standard Ts&Cs do apply but these will be reviewed depending on what is accepted.

A formalized project “kick-off” meeting would be arranged at the PORT ACCESS CONTROL where we would discuss in detail the solution proposed and determine exactly what will be deployed where, and also understand the areas of responsibility for all parties involved. The typical Project documentation will outline the following:

- Detailed scope of work
- Finalization of the design
- Responsibilities of all parties
- Expectations
- Deliverables
- Timings and milestones
- Financial aspects
- Requirements for communication
- Assumptions, concerns, etc.
- Exclusions
- Risks and how they will be addressed
- Personnel development/training
- Commissioning and implementation schedules
- Standards that must be complied with

... amongst other things



Once the plan is agreed and signed, final equipment orders will be placed on the manufacturers and the project planning will be completed.

Equipment installation will commence in accordance with the determined schedule as well as with the receipt of the equipment.

Once installed the system will be commissioned.

All training will then be finalized to ensure that staff are fully apprised of the operational and support issues.

The system will then be “made live” and operationalized.

Final project sign-off will then take place.

## 9 EQUIPMENT Considerations

**System description:** *Full-featured vehicle access control system with license plate reading software linked to facial identification and verification.*

Item	Qty
<b>PC</b>	
P4, 3G Hz, 512MB RAM, Windows XP	7
19" SVGA Monitor,	4
Keyboard and Mouse Switch	4
Cabling per metre, supply and install	4
Commissioning	1
Software to integrate LPR to FRS	1
<b>SUB-TOTAL</b>	
<b>NPRS</b>	
ART's LPR identify vehicles by a combination of color, shape, texture and license plate.	
I-Cube Stand Alone System	0
I-Cube SEE ROAD LPR Software (1 site, 1 lane) mono - Inc. Dongle, Lic,	0
I-Cube SEE ROAD LPR Software (1 site, 1 lane) STEREO - Inc. Dongle, Lic,	4
I-Cube SEE TRAFFIC (narrow lane, 1 See Traffic Head / lane)	0
I-Cube SEE TRAFFIC (wide lane, 1 See Traffic Head / lane)	0
I-Cube DLL LPR Software (1 site, unlimited lanes) - Inc. Dongle, Lic,	0
GEOVISION LPR Software 2 lanes @ 5 cameras	0
Frame Grabber Card	4
I/O Cards (7 lanes x 2 inputs = 14 @ 4 input)	4
LPR cameras REG LED 7M	0
LPR Camera I-CUBE Camera IR	0
LPR Camera ZC NH 403NP Day/Night 480 TVL Camera 12v/24vac. Day-colour, Night B-W.	24
5-50mm VF A/I Video drive Lense	24
GH - 24 Housing IP 68 with heater and wall bracket	24
Loop Controller	24
RELAYS - 5VDC 30 MA	24
On site installation and support	24
Remote management software for LPR	1
LPR Software Config	4
Training	4
<b>SUB-TOTAL</b>	

### V ideo

Facial Capture camera Lense 3,5mm	6
Push button for facial capture	6
5-50mm VF A/I Video drive Lense	6
UL Mini IR Illuminator 75W 10 Degrees	
IR illuminator PSU 12Vdc Linear	0
Daynight Switch for IR Illuminator	0
GH - 24 Housing IP 68 with heater and wall bracket	6
24VAC PSU 2A	6
Sundries	1

**SUB-TOTAL****Video Installation**

Camera installation incuding back box , rawbolts, focusing and setup	24
RG59 installed	24
RG59 Crimp connectors	24
Cable Cabtyre 3 core 1 mm Installed	24
Cable Cabtyre 3 core 2.5mm installed	24
Sundries	1

**SUB-TOTAL****Rack and UPS**

2 KVA 2hrs Backup with manual override	4
25U 19" rack, 800 deep. Keyboard tray and keyboard included. 3 x modem trays. 10 x dedicated power supplies. 2 x fans. 1 x brush tray.	4
Rack preparation	1
Sundries	1

**SUB-TOTAL****Digital Video Recorder**

Digital recorder (Geovision) - 16 input card	4
IO Card & Contact Boxes	0

**SUB-TOTAL****Containment and PSU**

25mm bosal installed /m	24
204 Box	24
204 Box mounting kit	24
20 mm adaptaflex	24
20 mm adaptaflex connectors	24
Electrical sub db installed Dirty power	24
Electrical sub db UPS with 16way box and CB's	24

---

Sundries	1
----------	---

**SUB-TOTAL**

**Electronic Display**

Display Board software	3
Display Board, exluding installation	3
On site installation and support	1

**SUB-TOTAL**

**WIRELESS COMMUNICATIONS**

Base Station	1
Connector to base station	6
PC Board	6
Install	

**SUB-TOTAL**

**Facial Identification**

Software (XP & 2000) to compare Facial images resulting in 12 closest matches	1
List Price for FRS Discovery Server software	1
List price for FRS Client Application	6
DB of less than 10 000	1

**SUB-TOTAL**

<b>Contingency and Project Management</b>	12
---	----

**MAINTENANCE**

Based on a 24 hrs turnaround (per month)	12
--	----

---

**Totals**

---



**Conditions**

- All prices are quoted in US DOLLARS and are subject to change.
- Proposal is valid for 90 days after which the pricing and product availability may well have changed.
- Neither installation nor commissioning has been quoted due to the unfamiliarity with the environment.
- Maintenance will be quoted separately.

**9.1 Acceptance**

**Customer Acceptance**

CUSTOMER: \_\_\_\_\_ VENDOR: POWER AUTOMATION

Signature: \_\_\_\_\_ Signature: \_\_\_\_\_

Name: \_\_\_\_\_ Name: \_\_\_\_\_

Title: \_\_\_\_\_ Title: \_\_\_\_\_

Date: \_\_\_\_\_ Date: \_\_\_\_\_

Specific considerations

Please sign and fax this page to POWER AUTOMATION

Dawa Sewbalak

**Power Automation**

E-Mail: [power.auto@intnet.mu](mailto:power.auto@intnet.mu)

**9.2 Standard Terms and Conditions**

Available on Request



## 10 Rental Option

### 10.1 BENEFITS OF POWER AUTOMATION RENTAL

Many of our customers ask whether it is better to buy **Cash or Rental**. However when buying high tech electronic equipment one has to remember that with today's pace of development that obsolescence needs to be taken into account. Because the equipment is computerized and networked we are totally dependent on the likes of Microsoft. This means that the **average lifespan of computerized equipment is 3 Years**. The receiver of Revenue has accepted this; hence all computer equipment is depreciated over a 3-year period. The present **trend for the increasing cost of importing such technology is averaging between 20-30% per annum** and does not make it financially viable to purchase a new system every three to four years. This is a conservative estimate and is due to a number of factors such as the poor exchange rate. It is therefore **not recommended to pay cash** for a hi-tech system like this as the capital will be tied up in a technology that has little equity and will be superseded within a three year period.

Due to the rapidly advancing nature of the computer technology used in our systems it is our policy to Rent our own locally developed and manufactured systems that will continually keep our customers abreast of the latest developments at affordable Rand based rates. This is achieved by phasing in minor software upgrades over the Rental contract period. We will however offer an **entire software and hardware upgrade after the initial three-year period**. To achieve this POWER AUTOMATION will cancel the outstanding twenty-four rentals on the old agreement upon acceptance and approval of a new five-year rental agreement, which will be kept at an acceptable and competitive rate. Whereby the latest updated system will then be installed.

The choice of a 0% or 12% escalating Rental agreement remains your choice. However as this is a balloon rental the **end total is the same**. It therefore does not give any benefit to pay the higher non-escalating rentals in the beginning due to the fact that we will be upgrading the system at the three-year period. Furthermore due to the fact that the goods remain the property of POWER AUTOMATION and do not become an asset to the customer there is no point in paying off the goods. Unlike the traditional lease rental, which reflects as a liability on the customers' balance sheet, the POWER AUTOMATION Rental is a **pure off balance sheet operating expense, which is 100% tax deductible**. This **alleviates the admin burden** of financial asset management, and depreciation, and furthermore frees up much needed capital and existing PORT ACCESS CONTROL facilities for better use within your business.

Quote from the September 2002 issue of UPFRONT

*".... Computer equipment in particular is the most rapid depreciating asset in South Africa. .... Market used equipment and it becomes understandable why most financial institutions attach a zero value to all used digital equipment."*

## 11 Conclusion

POWER AUTOMATION will supply and install the latest digital video technology, including advanced license plate recognition linked to biometric facial verification, identification and recognition. The latest LPR technology will be provided as a tool to verify entry and possibly identify an unknown person if they appear in the database. We believe that the POWER AUTOMATION solutions will grab the attention of all role players, leading to the focus on productivity, damage reduction and increased information flow, allowing a safer environment.

We deliver ROI-driven solutions that leverage video and control technologies to increase profit by eliminating inefficiencies and unproductive resources. We also provide customers an efficient way to secure their business environment, reduce costs and ultimately drive profit. Information Technology has become so integral

to success that it is now not only a support function, but could play a proactive and vital role in realising the business role. We offer technology solutions and services that allow customers to efficiently integrate, manage and maintain their people, processes and assets. Our adaptive infrastructure becomes increasingly critical to business success, balancing agility, robustness and affordability. By understanding the problem, we can address the solution. By reviewing what is occurring around the world, and customising this to your specific needs, we provide a complete solution.

The cost of technical solutions to maintain the gap ahead of the competitors, and to continue fighting crime is expected to keep rising steadily over the next few



years. To compete for investment dollars, we allow you to employ techniques like infrastructure pattern matching (reusable design), infrastructure impact assessment (analysing reuse), predictive cost modelling (total cost of ownership and budgeting), and application subscriptions (service-level-based packaging). Moreover, users cannot afford to wait until full deployment for a quantifiable return on investment. Each phase in the installation is justified by its own standalone ROI. Moreover, look closely at the effect the shift to the proposed infrastructure will have on near- and long-term infrastructure efficiency, image and customer satisfaction



## Appendices

## 12 Introduction - Role Players

### 12.1 Introduction

The role players involved with the selection and implementation of an integrated LPR system, which can involve security, EDUCATIONAL association, marketing and CCTV surveillance systems, need to involve all departments. However, the role players affected have a variety of criteria they might apply to the selection of a solution. Within the PORT ACCESS CONTROL there are at least four primary areas that would be affected by the introduction of facial recognition monitoring techniques. These are:

- Marketing (improving the experience of the visitors by recognising important guests);
- Security (ensuring the safety of people and property);
- Operations (LPR systems have a crucial role by speeding up identification); and
- Legislative (identification of any threat to the EDUCATIONAL FACILITIES by thieves, terrorists or con artists).



### 12.2 Marketing

The marketing department could use these proposed solutions to enhance the brand building experience to the benefit of the EDUCATIONAL FACILITY. This would build visitor confidence; loyalty and satisfaction, lower marketing costs, increase margins, and provide an opportunity for brand extension (Schrage, 2003). The LPR techniques must be able to be used to increase the loyalty of the users of the EDUCATIONAL FACILITY. Please see the MBA dissertation (Casino Exclusion Technique Exploration - Framework Development by Barry T. Dudley) for detailed views of this role player (Send e-mail to [mba@i-cube.co.za](mailto:mba@i-cube.co.za) to request a copy. A PDF file of 2MB will be sent to your E-Mail address).



### 12.3 Security

*Example of Cape Access Control*

The concerns of security are often at odds to the rest of the role players. Is Khayaletu Makhotyana (in the figure below), making the best utilisation of limited resources? Currently security places a high emphasis on the reaction to events, rather than being proactive.

We believe that the proposed system can be spark, which could propel security, to become a greater strategic ingredient. Rather than reacting to outside forces, the security department could lead the way in solving the problems. Tradeoffs exist among product and process choice versus the longer-term operating choices regarding quality, efficiency, schedule, and adaptability (Adam & Ebert, 2001). The first users of these LPR systems in South Africa have already successfully applied, managed and maintain a solution, thus earning the respect of all the role players.

Throughput rate requirements for both enrolment and operation will affect the successful implementation. Almost all systems require enrolment, with some techniques requiring multiple enrolments. One will have to provide personnel for the use of the exclusion technique during operation, to observe or operate the system and users.



### 12.4 Operations

The application of security and monitoring techniques as proposed will lead to an increase of core competence. The security department needs to grow with the use of surveillance equipment, this is a subsystem and the combination of skills, processes, technologies and assets which come together within each subsystem to confer sustainable, repeatable and unique competitive advantage. It is essential to plan and execute new categories, which continue to build and reinforce these competences? The solution proposed allows this to occur, growing as the security department gains confidence in the equipment and the application thereof. The security department has to remain current with the external threats posed, such as tips on how to avoid detection by the surveillance cameras (Tamburin, 2003).

Please see the MBA dissertation (Casino Exclusion Technique Exploration - Framework Development by Barry T. Dudley) for more information.



*Cameras used to potentially recognise thieves and prevent illegal entry.*

*Current system that allow abuse*

### 12.5 Legislative

EDUCATIONAL FACILITIES need to do everything in their power to prevent thieves from entering the EDUCATIONAL FACILITY. EDUCATIONAL FACILITIES who do not take their public role seriously are quick to feel the backlash, with serious consequences against those who are found to have a problem. Implementing the proposed solution allows the PORT ACCESS CONTROL to show that they are doing everything in their power to prevent criminals, con artists or terrorists from gaining access.

Please see the MBA dissertation (Casino Exclusion Technique Exploration - Framework Development by Barry T. Dudley) for detailed review of all exclusion techniques (Send e-mail to [mba@i-cube.co.za](mailto:mba@i-cube.co.za) to request a copy. A PDF file of 2MB will be sent to your E-Mail address).

## 13 LPR Scope Of Work

To supply and install a digital video surveillance and management system, based on LPR and facial recognition, that will provide authentication of the vehicle and video images of the entry and exit of all vehicles, the driver, vehicle as well as general surveillance of the access area. The LPR system would replace security manually entering the data. The LPR information would come from an image captured on the DVR, via DDE. All drivers' facial images and vehicles would be captured, allowing for immediate recall and review. The LPR system allows the driver to be identified immediately if the guard has any cause for concern.



FIGURE: Currently existing parking LPR solution

Sample of system accuracy where read seq. is set to 100%

### CHEP LPR RECOGNITION RESULTS

	%	Number
Confirmed Recognition	99.90	18136
Recognition per event	95.5	
Entry event	1.5	290
Hyster triggers	1.5	290
Dive round triggers	0.8	160
Unknown reason for trigger	0.0	2
Entry recognition	0.0	3
Incorrectly ID	0.1	19
REVERSING	0.4	70
Vehicle driven out while 2nd vehicle on loop	0.2	30
MISSED DUE TO SYSTEM OFF		5
<b>TOTAL</b>	<b>100.0</b>	<b>19000</b>

### 13.1 Full description of system topology offered

Field LPR engines connected to the LPR cameras by frame grabbers (6 inputs) capture the images and process the information from the Parking Garage, the result of license plate recognition and facial and vehicle colour capture. This information and the images are transmitted to the central server, by the network, immediately being available for review and reaction by any of operators at the operator stations.

Each field system can operate totally independently, and will update the central server as soon as this becomes available. As such, the HOT list is downloaded to each field PC, so no illegal / unwanted vehicles might use the weighbridge.



**System Architecture:** The License Plate recognition product is a turn-key system comprises of the following elements:

- a **PC Pentium** running Windows 98/NT/2000
- **See/Car DLL** - which is used to analyse the images and extract license plate string.
- Camera/Illumination unit to capture the images (See/Car/Head –LPR camera and illumination unit)
- a **Frame Grabber** - which captures the images from the camera units (handles 1-6 lanes)
- **I/O card** – input/output board with multiple I/O discrete lines. This board supports the sensors, illumination control and optional gate-open signal. It is connected via a cable to a terminal interface board with easy connections and indicator lights.
- **Sensors** to indicate the presence of the car (a sensor for each lane)
- **See/Lane** The See/Lane Windows application interfaces the hardware elements (frame grabber, camera/illumination unit (s), IO card and sensor). It controls the illumination, reads the video inputs and passes the images to the DLL in order to obtain the recognition results. The application displays the image and recognition results. It then exports the results using serial communication, messages or disk files. Its man-machine interface supports on-line setting control, which can easily adapt the application to various types of configurations.



The camera is triggered by the loop in the road

SeeParkClient is an application that is used to monitor a parking lot (secured area with a specified number of entrances and exits). This application records the entrances and exits in a simple flat database, and uses the information to match events using the POF string.

To share the results (pass the remote data to the centers), an additional utility - **SeeData** - is used to pass the recognition results and copy the image files to the Center. The product runs on basis of TCP/IP and sends the data across the network. It is consisted of two parts: one running on each remote unit (as a background application), while the other part runs on the Center Server (also as background application). The product can also send back commands from the Center to any remote lane in order to activate a sensor or command to open a gate.

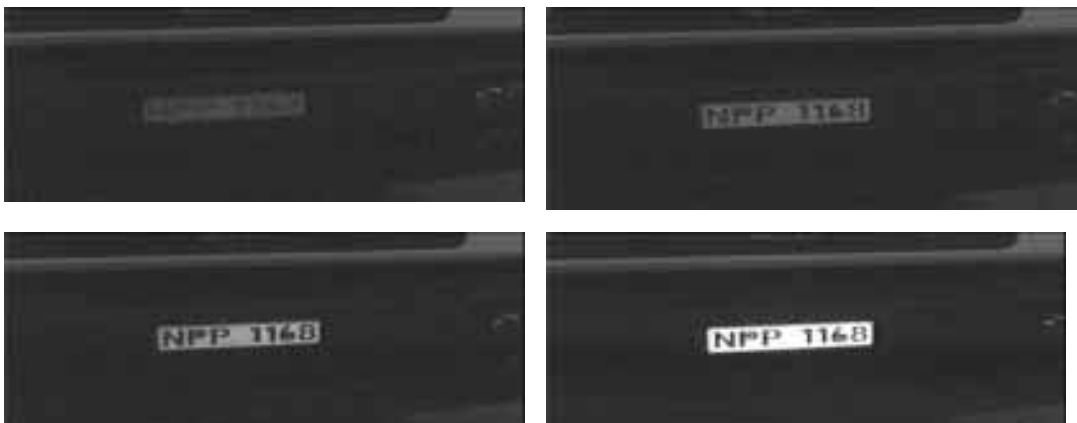


To simplify the maintenance of our products, our **SeeMonitor** tool monitors the operation of cluster of SeeLane and provides a quick view of the operation (in green/yellow/red status). The status is determined by automatically checking the Windows' application event logs (where our products log information, warnings and errors). These events include possible failure of hardware units, application problems and decrease of recognition results under acceptable levels.

**SeeMonitor** also provides various performance graphs for each remote unit, and a multiple view of the units. These graphs assist in the fine-tuning of the system. In the following example the graph of the horizontal center of the ID marking is shown as a histogram, which can be used to verify the correct settings. The graphs are available on-line and generated automatically, thus simplifying the analysis of the operation of the system.

**SeeService** is an additional utility that "keeps an eye" on the recognition units (SeeLane or SeeGate application). In case it stops to respond (rare cases...) it resets the application and restarts. The utility also checks for updates in the Server, and if there is a new file revision - it automatically updates the application.

To simplify the installation, a calibration tool (**SeeCal**) is available as a very useful tool. The tool shows the camera video, displays brightness/contrast graphs, and enables manual control over the I/O card controlled illumination.



*IR being used at night to highlight the PLATE*

### 13.2 Sample sequence of operation

The timing of the system (per lane) is described below: ENTRY

#	The VEHICLE	The system	Time
1	Vehicle enters ENTRY LANE and approaches the sensor.		
	In idle, waiting for the sensor activation		
2	Passes over loop and Activates the sensor Nortec loop detector (see documentation)	Switches to capture mode.	0
3		Captures one or more images into memory	~50 msec per image capture
4		Changes the illumination; Captures one or more images into memory; Repeats the illumination change	~50 msec per image capture
5		Calls DLL on one or more images	
6		Identifies the car	+ ~80 msec per

			image identification
7		Logs, displays, transmits the Identification to the FACIAL VERIFICATION system which will check the database, via DDE. Checks the database for vehicles in the BLACK list, which will cause an alarm.	
8	Stops when fully at card reader (if installed)	Person swipes and IF EXISTING CARD confirms face via verification. If not enrolled, will enrol, taking full frontal facial images and another image of the VEHICLE COLOUR	~40 msec for a single image capture
9	Drives on	Access card / issued ticket now links facial images, car colour, license plate and date and time and lane.	
10		Goes to Idle	About 0.5 second from the car entry (a typical setting)
11	Next Vehicle triggers the sensor		

The timing of the system (per lane) is described below: EXIT

#	The VEHICLE	The system	Time
1	Vehicle enters EXIT LANE and approaches the sensor. In idle, waiting for the sensor activation		
2	Passes over loop and Activates the sensor Nortec loop detector (see documentation)	Switches to capture mode.	0
3		Captures one or more images into memory	~50 msec per image capture
4		Changes the illumination; Captures one or more images into memory; Repeats the illumination change	~50 msec per image capture
5		Calls DLL on one or more images	
6		Identifies the car	+ ~80 msec per image identification
7		Logs, displays, transmits the license plate recognition to the FACIAL VERIFICATION system which will confirm this via the pre-enrolled template via DDE. Checks the LOCAL database for vehicles in the BLACK list, which will cause an alarm and NOT allow boom to open.	
8	Stops when fully at card reader (if present)	Takes a full frontal facial image for facial verification and another image of the VEHICLE	~40 msec for a single image capture
9	If the transaction is allowed system proceeds to open boom.	If face or license plate or card or car colour does not match the information on the ticket, control room is alerted and presented with facial image and general car overview for comparison. Operator makes decision which is recorded.	
10		Goes to Idle	About 0.5 second from the car entry (a typical setting)
11	Next Car triggers the sensor		

### 13.3 Suggested LPR Procedure:

#### ENROLMENT:

#### EXISTING EMPLOYEES:

The existing card owners would have their license plates entered into the existing database and linked to their name, facial verification and car details. The member's database would be locked, allowing only authorised users to add new members.

When the cardholder vehicle is seen the system will expect the card and facial verification associated with them, also logging them, with details of time of entry and name associated the license plate. The optional SEE SPEAKER system allows the guards to immediately learn who is who and address each regular parking person by name.



#### CASUAL VISITORS

When CASUAL VISITORS were expected, their details could be entered prior to arrival so that when they arrived they can be linked to an access card. If they were not on the system, the driver would drive up to the entrance, a picture of the plate would be captured, OCR would occur, after which the driver would do facial verification, linking the printed ticket to the license plate.

The natural process of e-mailing, calling or filling a simple completed VISITOR application document directly to the system means that when a casual VISITOR arrived at the counter their license number is automatically entered into the custom VISITOR system, and their authorised record would appear. Access to the correct areas with the correct expiry is automatically issued.

#### ENTRY USE

#### EMPLOYEES:

The existing long-term employees would drive up to the gate (any of X). The LPR system would capture the plate and if the plate were in the database the LPR system would link the plate to a card, if this matched, this would then open the gate. The DVR system would then link the vehicle license plate to the drivers face and the vehicle. If there was any concern the guard would investigate past events to see the driver and car matched the plates.



## VISITORS

Pre-registered VISITORS would be identified by LPR, which would transmit the details to the facial verification reader via DDE, TCP/IP or RS232. The biometric system would link the VISITORS info to the license plate and if required a parking ticket, and allow the boom to open.

## EXIT USE

### EMPLOYEES:

The existing long-term employees would drive up to the exit gate. The LPR system would capture the plate and pass this information to the facial verification and DVR system. If the facial verification matches the enrolled template and the parking ticket is correct, the boom will open. The DVR system would then link the vehicle license plate to the driver and car seen on the cameras.

## VISITORS

All VISITORS exiting would be identified by LPR, which would transmit the details to facial verification reader via DDE, TCP/IP or RS232. If the license plate, the VEHICLE ticket info and the biometric ticket issued match, the boom would open.

If not, the guard would investigate.

All video images will be digitally recorded. Video images can also be transmitted to the main office if required. Transmission of the camera images to a remote monitoring control room will be possible.



## 13.4 Schedule Of Equipment Specifications

See attached EXCEL file

## 14 LPR Equipment Quote

TO PROVIDE FIXED BLACK & WHITE CAMERAS WITH 16 MM FIXED-IRIS LENSES, AND BRACKETS

SeeCarHead (s): Integrated Camera/Illumination unit(s) housed in a weatherproof enclosure.

- Power supply for SeeCarHead units (input: 110-220 VAC)



Figure See/Car/Head

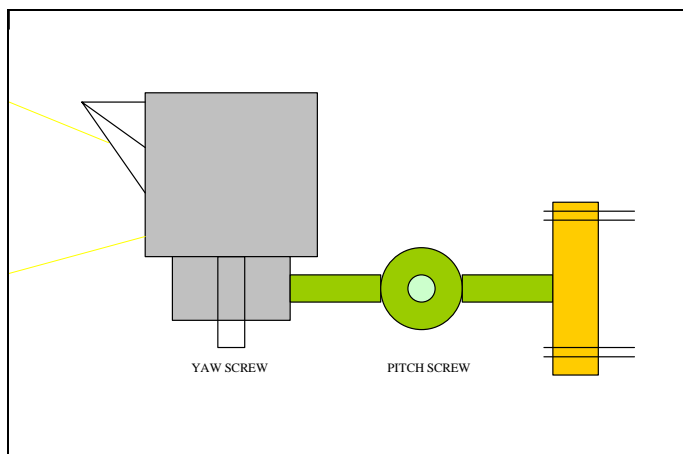


Figure: Pitch & yaw screws



The standard Infra-Red model specifications are:

**Camera:**

- Sensor: CCD 1/3" B&W CCIR
- Scan: 625 Line interlaced
- Resolution: 380 TV lines
- Shutter: 1/1000
- Power: 9-16 VDC 100mA
- Lens: F1.2-16C / 8,12,16 mm

**Illumination:**

- Spectrum: a. near Infra-Red (for most Countries)
- Angle: 30
- Intensity: 3 levels pulsed
- Power : 12VDC , 3A pulsed
- Effective Range: 8M (reflective plates) to 4.5M (non-reflective)

**Physical:**

- Case: Enforced Poly-Carbonate, UV protected
- Standard: IP 65 , weatherproof
- Temperature: -10 c to +50 c
- Degrees of freedom: 2 (left/right, up/down)
- Attachment: 2 x 8 mm screw
- Dimensions: Front: 150x150mm, Depth:135mm+35mm hood, Arm: 160mm
- Drawings: can be downloaded from support page

**Electrical:**

- Power: Power Supply: 3A 15VDC
- Inputs: 2 lines TTL (3 levels of intensity + off)
- Output: Composite Video 1Vp-p / 75

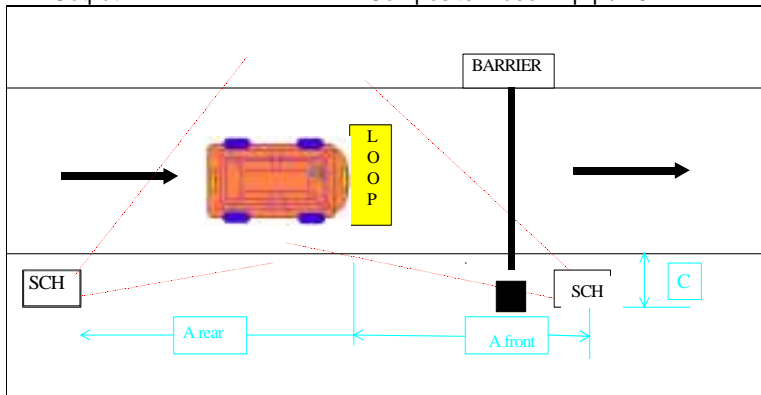


Figure Front & Rear installation (dual cameras per lane, shared activation)

- Input/Output control card (including flat cable and terminal block with cover)

TO INSTALL three (3) PC,19" SVGA MONITOR.

### Licence Plate Recognition

Date	Time	RegNo	Ln	Result
20040801	11:27:28	KPP03556P	3	Alarm
20040801	11:28:28	CVV23064	3	Alarm
20040801	11:31:24	3M414270	3	OK
20040801	11:32:06	3M414270	3	OK
20040801	11:33:52	3PH98820P	3	OK
20040801	11:33:58	33AL225	3	Unknown
20040801	11:34:02	3PH92350P	3	Alarm
20040801	11:34:05	3PH94500P	3	OK
20040801	11:34:05	3PH92350P	3	Alarm
20040801	11:34:07	3L88710P	3	OK
20040801	11:34:08	33AL225	3	Unknown
20040801	11:47:19	3M1122298P	3	Unknown
20040801	11:47:19	3M1122298P	3	Unknown
20040801	11:47:17	3M1122298P	3	Alarm
20040801	11:54:37	33A1005	1	OK
20040801	11:54:38	33A1005	1	Unknown
20040801	11:56:21	3M202170	1	OK
20040801	11:56:28	3M202170	1	Unknown
20040801	11:56:28	3M202170	3	OK
20040801	11:56:29	3M11840P	2	Unknown
20040801	11:56:28	3PH7870P	4	Alarm
20040801	11:57:38	3PH0490P	1	OK
20040801	11:12:14	3PH0490P	1	OK
20040801	11:12:24	3PH02170	1	Unknown
20040801	11:12:32	3M11840P	2	Alarm
20040801	11:12:34	3PH7870P	4	OK
20040801	11:14:05	3M202170	3	OK
20040801	11:15:02	3PH0490P	1	Unknown
20040801	11:16:18	3M11840P	2	Alarm
20040801	11:16:13	3PH7870P	4	OK

**PKT8570P Lane 4 16:15:12** ●

**NJM1840P Lane 2 16:15:06** ●

**ND282178 Lane 3 16:14:56** ●

**PHC0490P Lane 1 16:15:02** ●

**Alarm Queue**

Date	Time	RegNo	Ln
20040801	16:15:02	PHC0490P	1

**Unknown Queue**

Date	Time	RegNo	Ln
20040801	16:15:02	PHC0490P	1

**Camera Errors**

Date	Time	Cam
------	------	-----

- AN UNINTERRUPTED POWER SUPPLY FOR THE SERVER.
- **OPTIONAL EXTRA - ELECTRONIC DISPLAY-**

<i>Model</i>
1 x MS 24/6-2L (1000 mcd)
• This unit consists of 2 lines,
• With 24 characters per line
• Colour : RED LED's
• IP Enclosure

The PORT ACCESS CONTROL welcomes



INTEGRATION OF ALL ITEMS DETAILED.

## 15 Software Quote

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

### I-CUBE Facial Identification Client

Microsoft® Windows® 2000 Professional (Service Pack 4) or Microsoft® Windows® XP Professional

- 1 GHz Pentium 4 Processor
- 128 MB RAM
- 10 GB HDD
- CD-ROM Drive
- WDM – compatible video capture device

### I-CUBE Facial Identification Server

Microsoft® Windows® 2000 Professional (Service Pack 4) or Microsoft® Windows® XP Professional

- 2.6 GHz Pentium 4 Processor
- 512 MB RAM
- 160 GB HDD
- CD-ROM Drive
- WDM – compatible video capture device

The performance of the I-CUBE Facial Identification CLIENT PC is subject to at least an ISDN connection to the central server.

The I-CUBE Facial Identification requires a skilled operator who has either been trained or has read and understood the I-CUBE Facial Identification user manual.

The software will allow the following information to be added to the database, both locally and remotely:

Information	NPRS Use
VEHICLE DRIVER(s) Name	Yes
Date of Visit	Yes
Vehicle Registration Number	Yes
Ticket & Biometric Facial CAPTURE	OPTIONAL
Vehicle Colour	The DVR system will capture vehicle colour.
Driver Face	The DVR system will capture the drivers face.

SeeLane software application package, including integrated SeeCarDLL recognition engine



SeeLane Product user's license

POWER AUTOMATION System Scope of Supply (see product leaflet for description and performance)

SeeLane is a PC-based multi-lane LPR system designed for low speed traffic. The SeeLane system includes both hardware and software, and can accommodate either one camera per lane (standard configuration) or two cameras per lane (stereo vision) for added reliability and security.



Typical SeeLane Configuration

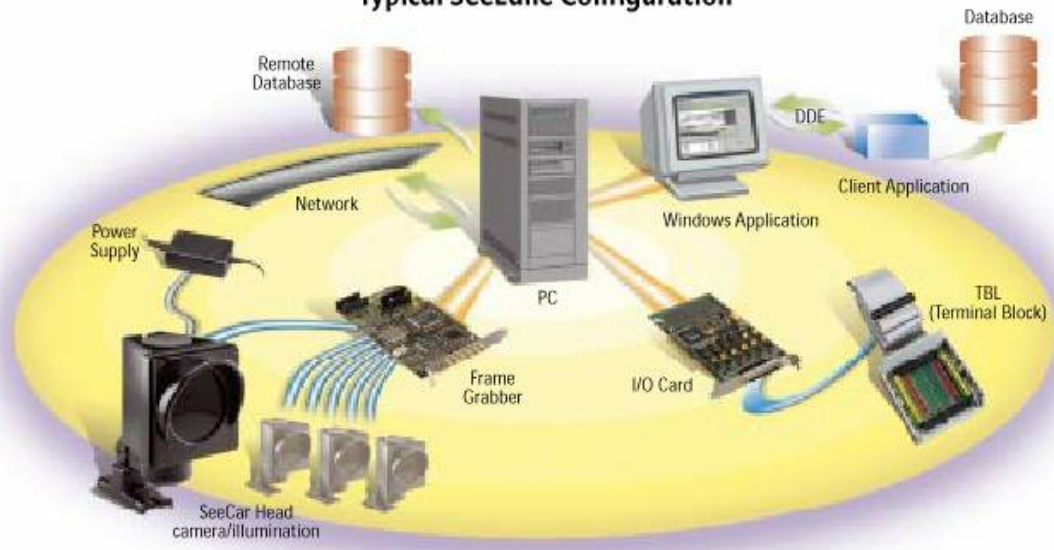


Figure See/Lane configuration

Event Code	Event Code	Event Code	Time	Processed	Time	Vehicle
11	MP1001	NUM3222	2005-05-11 10:10:10	Yes	2005-05-11 10:10:10	2005-05-11 10:10:10
12	MP1002	NUM3222	2005-05-11 10:10:11	Yes	2005-05-11 10:10:11	2005-05-11 10:10:11
13	MP1003	NUM3222	2005-05-11 10:10:12	No	2005-05-11 10:10:12	2005-05-11 10:10:12
14	MP1004	NUM3222	2005-05-11 10:10:13	No	2005-05-11 10:10:13	2005-05-11 10:10:13
15	MP1005	NUM3222	2005-05-11 10:10:14	No	2005-05-11 10:10:14	2005-05-11 10:10:14
16	MP1006	NUM3222	2005-05-11 10:10:15	No	2005-05-11 10:10:15	2005-05-11 10:10:15
17	MP1007	NUM3222	2005-05-11 10:10:16	No	2005-05-11 10:10:16	2005-05-11 10:10:16
18	MP1008	NUM3222	2005-05-11 10:10:17	No	2005-05-11 10:10:17	2005-05-11 10:10:17
19	MP1009	NUM3222	2005-05-11 10:10:18	No	2005-05-11 10:10:18	2005-05-11 10:10:18
20	MP1010	NUM3222	2005-05-11 10:10:19	No	2005-05-11 10:10:19	2005-05-11 10:10:19
21	MP1011	NUM3222	2005-05-11 10:10:20	No	2005-05-11 10:10:20	2005-05-11 10:10:20
22	MP1012	NUM3222	2005-05-11 10:10:21	No	2005-05-11 10:10:21	2005-05-11 10:10:21
23	MP1013	NUM3222	2005-05-11 10:10:22	No	2005-05-11 10:10:22	2005-05-11 10:10:22
24	MP1014	NUM3222	2005-05-11 10:10:23	No	2005-05-11 10:10:23	2005-05-11 10:10:23
25	MP1015	NUM3222	2005-05-11 10:10:24	No	2005-05-11 10:10:24	2005-05-11 10:10:24
26	MP1016	NUM3222	2005-05-11 10:10:25	No	2005-05-11 10:10:25	2005-05-11 10:10:25
27	MP1017	NUM3222	2005-05-11 10:10:26	No	2005-05-11 10:10:26	2005-05-11 10:10:26
28	MP1018	NUM3222	2005-05-11 10:10:27	No	2005-05-11 10:10:27	2005-05-11 10:10:27
29	MP1019	NUM3222	2005-05-11 10:10:28	No	2005-05-11 10:10:28	2005-05-11 10:10:28
30	MP1020	NUM3222	2005-05-11 10:10:29	No	2005-05-11 10:10:29	2005-05-11 10:10:29

TO INCORPORATE ONE LOGGING SOFTWARE

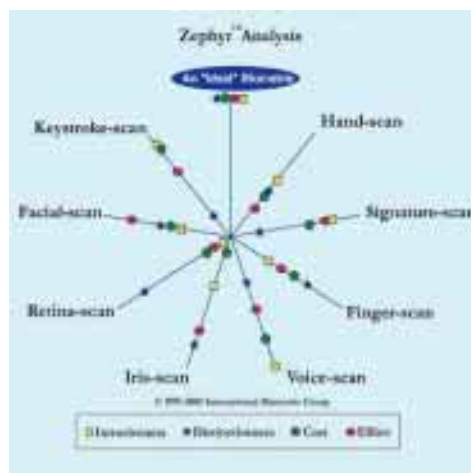
## 15.1 FACE RECOGNITION SYSTEMS

"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

### 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 CONFIRM 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](http://www.businessweek.com/technology/content/jul2003/tc20030722_2846_tc125.htm) .

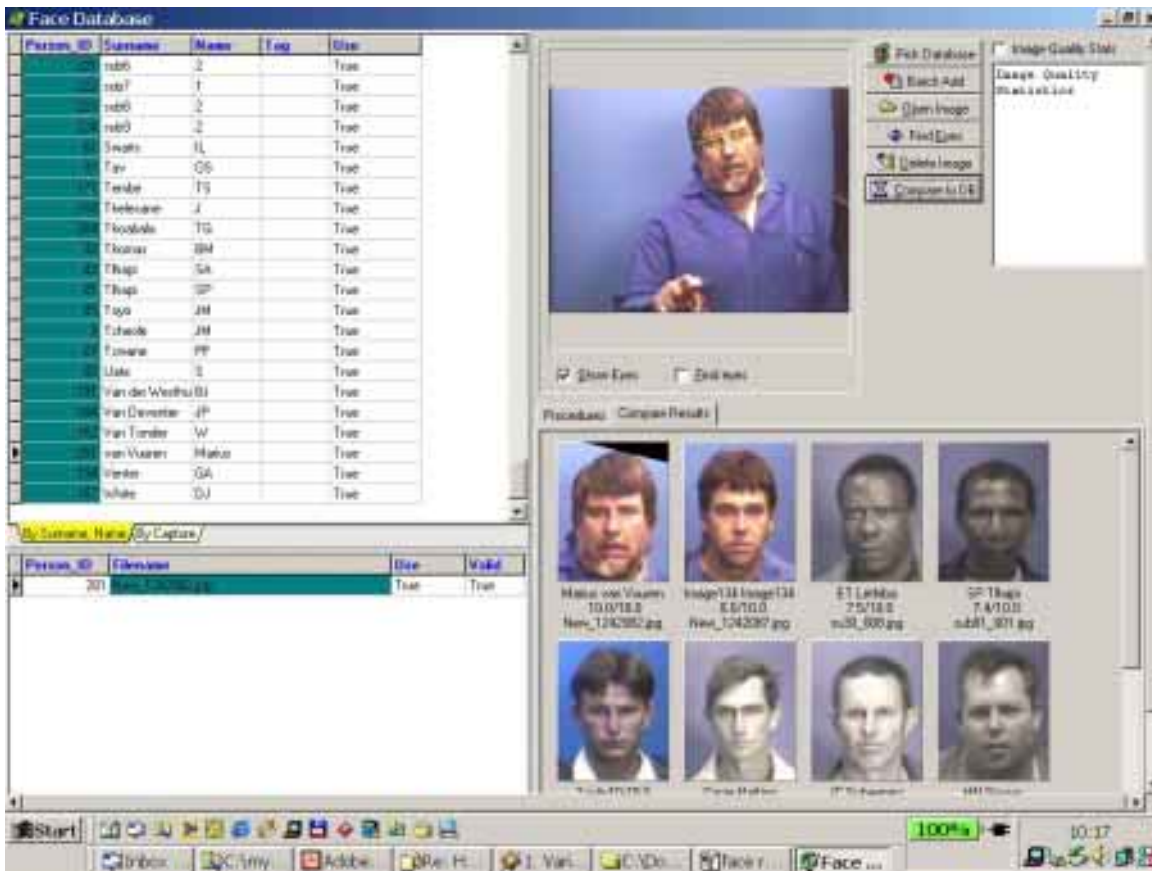
### Zephyr Analysis to determine the "ideal" biometric

New real time security alternatives are a reality today with the I-CUBE SYSTEMS lighting fast Face Recognition System. A leading developer of mission critical biometric solutions, I-

CUBE SYSTEMS is committed to leadership, responsiveness and unparalleled results. We are driven to empower our clients and partners to go beyond tradition to create new benchmarks for security. Accuracy is everything.

**Facial recognition used for identification.**

**Biometric Intelligence:** 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 surveillance. Such surveillance is most effective if the people you are trying to locate are not aware of its use. Audit trails left by an individual as he or she uses Casinos, car rentals, and any other services that require biometric authentication (i.e., possibly any activity that requires the use of a credit card, driver's license, passport, or any other major form of identification) could become a significant contribution to intelligence systems.



## 16 Privacy discussion

Discussion concerning the implementation of large-scale biometric systems always includes 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](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 in 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.



## 17 LICENSE PLATE RECOGNITION LINKED TO FACIAL VERIFICATION USER MANUAL

### CONTENTS PAGE

Terms and conditions of use

Normal Operation

Adding a user to the LPR database

Restricting access to a user in the LPR database

Adding a user to the FRS database

Restricting access to a user in the FRS database

VIEW HISTORY - Access the LPR LOG

VIEW HISTORY - Access the FRS LOG



Terms and conditions of use



is provided as a demo UNIT and does not comply with the final product.

Only users trained by POWER AUTOMATION can use this system.

Any DEMO of the equipment can only occur with the permission of POWER AUTOMATION and with POWER AUTOMATION present.

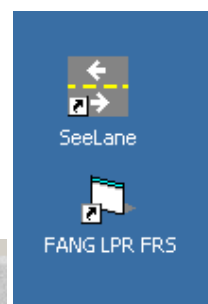


### NORMAL OPERATION

When the PC is started the required software, LPR FRS is automatically started. LPR begins to operate immediately, logging all vehicles and if the number plate is in the database, opening the boom.

To connect the Facial Verification to the LPR, click LPR LINK

Facial



FACIAL on the Front End.

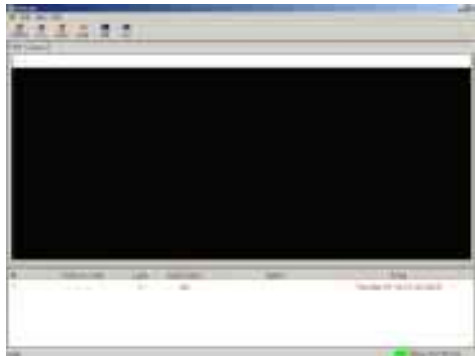
and

the

to

the

If the software is closed for any reason, select the following ICONS to being the LPR and FRS software.



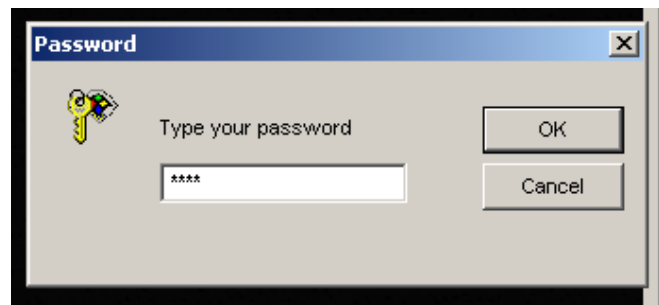
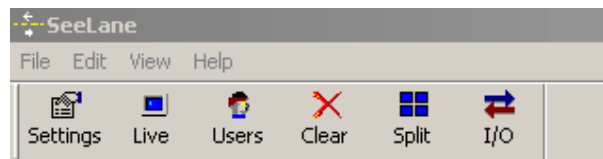
**LPR FRONT END**



**FRS FRONT END**

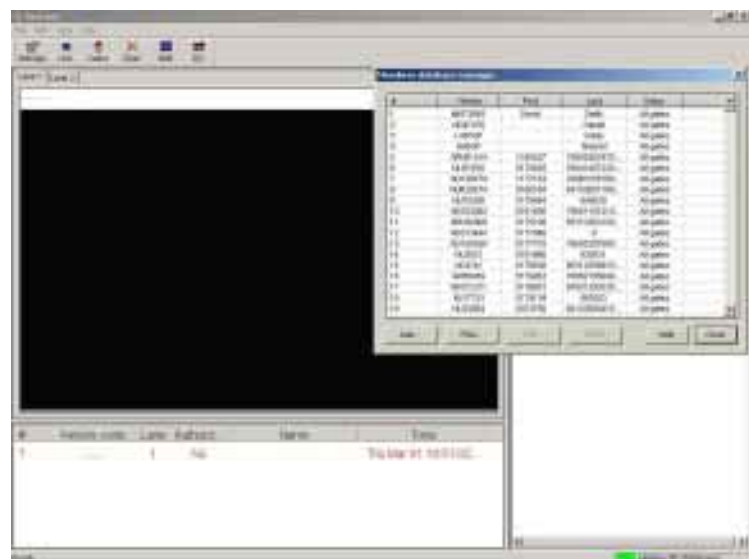
Adding a user to the LPR database

Select the users ICON by clicking on the person or by pressing F5 or by selecting EDIT USERS from the MENUE on the top of the LPR front end / screen.



In order to add a user to the LPR system you need to be an administrator, with a password.

Once you have typed in your password, you will be allowed access to the MEMBERS DATABASE MANAGER



**Authorized Members Database Manager**

View area:  
#



**A Sequential number within the members list (automatic).**

**Code**

The vehicle plate string. Used to determine if the recognized vehicle is an authorized member (and to optionally open the gate for this member).

**First**

Private name, or any other text of 32 characters maximum.

Used to identify the authorized member.

**Last**

Family name, or any other text of 32 characters maximum.

Used to identify the authorized member.

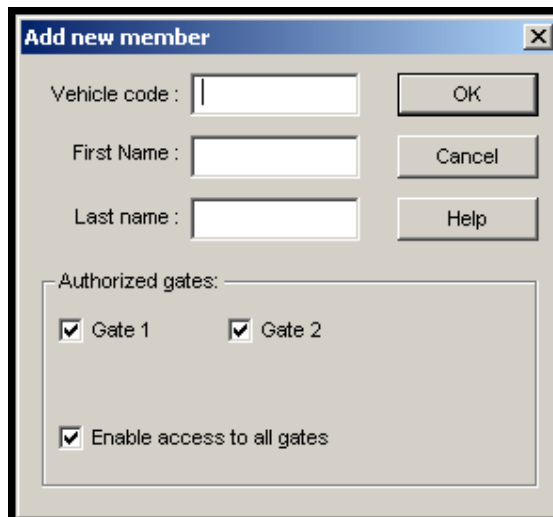
**Gates**

Specifies the gate number that the member can pass through when recognized.

Used to limit the rights of access to some vehicles.

Range: 1 to Maximum licensed lanes.

Default: "All gates", which grants access for authorized members to all gates.



One click on the top of each column will sort the list according to the subject for example click on sequential number will change the sort order from increasing to decreasing and vice versa.

Command buttons area:

**Add**

Add a record to the members list. A separate window will be open with the following fields:

Vehicle Code: The license plate as seen on the vehicle, without spaces

The First name of the driver

The last name of the driver

Gate one (1) is the entry lane and Gate 2 (two) is the EXIT lane.

**Find**

Find a record according to one or more of the following: Vehicle Code, First name or Last name. A separate window will be open.

**Edit**

Edit a record. This button is disabled. It can be enabled only by clicking on a specific record in the view area. Clicking on the Edit button will open a separate window (same window as Add new member) with the record details. It is possible to edit this record.

Another way to edit a record is double clicking on the record in the view area.

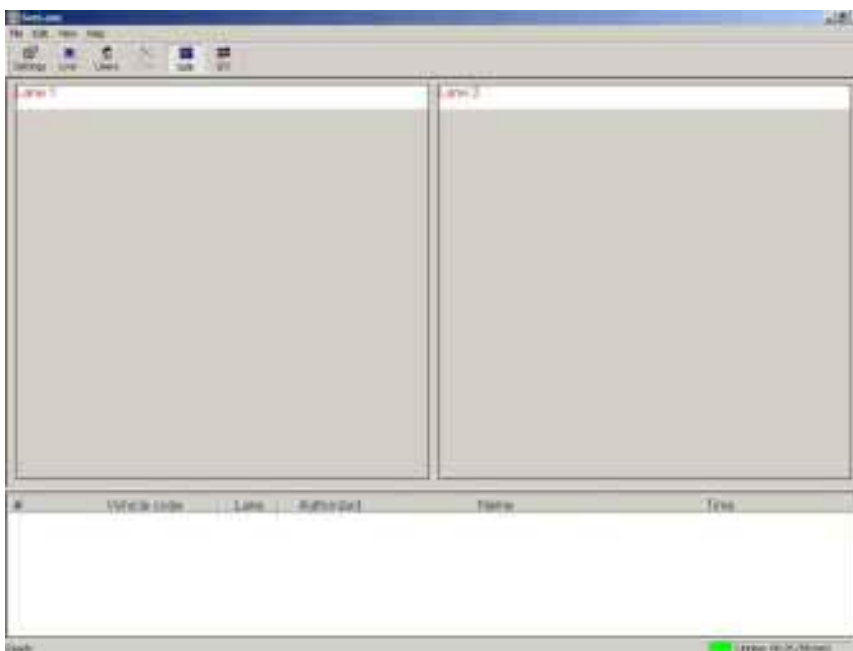
**Delete**

Delete a record. This button is disabled

It is suggested you do not delete plates but disable access to gates; hence you will always keep a record of all visitors and cars allowed access.

Two lane front end

Restricting access to a user in the LPR database



It is suggested you do not delete plates but disable access to gates; hence you

will always keep a record of all visitors and cars allowed access.

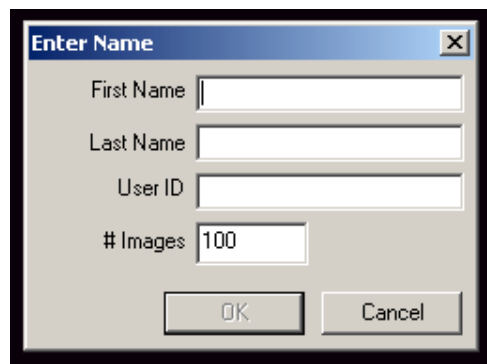
Adding a user to the FRS database

When adding a person the FRS system you HAVE to keep the SAME name and LICENSE PLATE number.



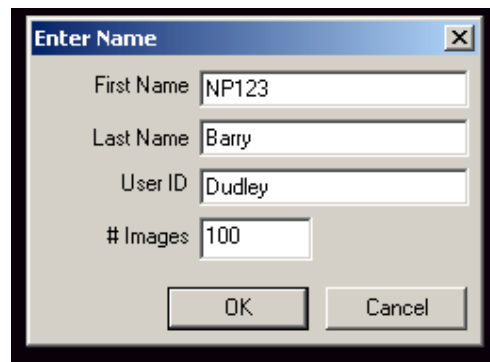
To enrol a person, click the enrol button.

This enrollment operation is used to either add a new user or append new enrollment images to an existing user. This operation collects facial images from video input and uses these images in the generation of the biometric template .



Fill in the SAME information as you entered from the LPR system.

**ENSURE THIS INFORMATION IS CORRECT.**



When you click OK the person will be captured, please ask them to be patient and they must be in their car, looking at the camera. If they wear glasses, please ask them to have them both on and off, please ask them to move and smile at the camera to ensure good images are captured.

Enter the User's first name into the First Name textbox and last name into the Last Name textbox.

- Enter the User's ID into the User ID textbox.
- Enter the number of facial images to be captured into the # Images textbox. The default value is 100.
- Click the OK pushbutton.

During the enrollment process, facial images of the user are collected and added to the FRS database. The progress of the enrollment operation, in terms of number of facial images collected, is displayed as a green progress bar within the Confidence Window located above the video display area.

It is possible that fewer than the number images as specified within the # Images textbox may be collected during the enrollment operation. This will occur in the event that the enrollment timeout limit is reached. These timeout values may be modified through the Enrollment tab of the Options dialog (refer to Section 3.2.3).

When the image collection operation has completed, the following dialog is activated to provide manual review and deletion of the enrolled images. The Review Enrolled Images dialog provides the option to remove facial images either of poor quality or corresponding to the wrong individual. The user may scroll through the collected images using the < and > buttons. Images are removed one at a time by selecting the image and clicking the Remove pushbutton.

When the user is satisfied with the set of enrolment images, click the OK pushbutton to transfer the images to the FRS database and generate or re-generate the associated biometric template.

The system will collect facial images more quickly if the individual that is being enrolled physically moves, preferably by walking towards the camera. It is also preferable that the enrolled individual provide a range of head orientation and expressions that is typical of casual movement. Physical movement of the individual is useful in that these range of conditions occur naturally and that lighting conditions can be adjusted to vary significantly over rather short distances.

It is normal for people new to the system to stare fixedly at the video display during enrollment, without exhibiting any movement. To achieve optimal performance, you should create a situation in which the user is moving their head and walking naturally, as well as being exposed to some variance in ambient lighting conditions.

The system may also be configured to issue verbal commands to the user, in order to guide the enroll procedure

**Restricting access to a user in the FRS database**

It is suggested that one does not remove people from the Facial Database but just change the user ID or LICENSE PLATE DETAILS:

So if the Plate number was NP123 – change this to NP123PLUMBER OR NP123LEFT COMPLEX or NP123GUEST or NP123FIRED etc., depending on the reason they are removed from the system.

PLEASE REMEMBER that this DB is limited to 1000 users, the full system is not limited at all.



VIEW HISTORY - Access the FRS LOG

In order to view the history file, click on Event Viewer

The Activity Log Viewer displays the list of operating events that have occurred within the Discovery Client/Server installation. Provided within log is the time and date in which the event occurred, identity of the Discovery Client or Server machine, associated user name (if applicable) and the type of

The Activity Log also provides an image captured from the Discovery application at the time that the event occurred.

The events that are recorded and displayed within this log are as follows:

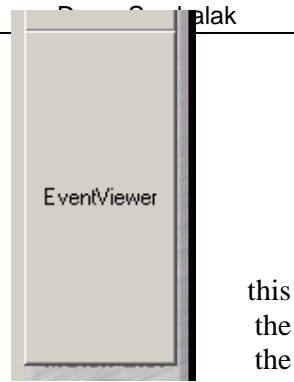
- Enroll Failure
- Enroll Success
- Reenroll
- Verify Failure
- Verify Success
- Classify Failure
- Classify Success

Multiple activity logs may be generated and viewed using the multiple document interface provided within the Activity Log Viewer. Each view may be filtered to list events by event time and date, computer name, user name and event type.

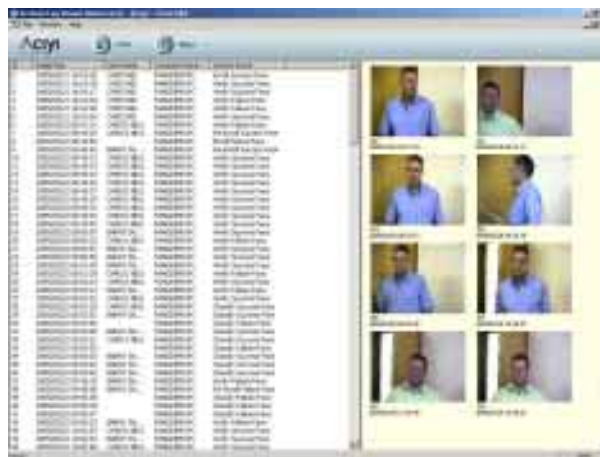
Any report contained within the Activity Log Viewer may be saved and restored from a binary file. The report may be also saved to a text file for import and processing by third party software.

The list of events provided within a window of the Activity Log Viewer can be saved to a text file for later processing. Note that the associated JPEG images are not exported when saving the selected activity log to a text file. To save an activity log to a text file perform the following operations:

- Select the window containing the activity log that is to be saved.
- Select the Save Text File menu item from the File main menu. A standard File Save dialog will appear.
- Enter the name of the file to which the activity log is to be saved. If an existing file is selected it will be overwritten.
- Click the OK pushbutton. Activity log files that are saved in text (ASCII) format are assigned a ".log" extension.



this  
the  
the  
event.



The list of events provided within a window of the Activity Log Viewer can also be saved to a binary file. Activity logs saved using this method store the associated images in JPEG format. Binary activity log files may also be reloaded back into the Activity Log Viewer, unlike the Activity Logs saved using the text file format. To save an activity log to a binary file perform the following operations:

- Select the window containing the activity log that is to be saved.
- Select the Save Binary File menu item from the File main menu. A standard File save dialog will appear.
- Enter the name of the file to which the activity log is to be saved. If an existing file is selected, it will be overwritten.
- Click the OK pushbutton. Activity log files that are saved in binary format are assigned a ".bin" extension.

Note that a portion of an activity log may be saved in either text or binary format by multi-selecting the activity events records displayed on the left panel and using the right-click pop-up menu.

Images that are displayed on the right panel of the selected window may be saved to JPEG files individually or through multi-selection. These file are saved using a file name that is generated from the corresponding textual data displayed in the left panel of the window, as follows:

DISCOVERY\_[Time]\_[User  
Name]\_[Computer Name]\_[Activity]

To save the selected images to JPEG files, perform a right-click operation on a selected image and click the Save Image menu item.



**VIEW HISTORY - Access the LPR LOG**

1. Overview

-----

This application is a new Client application for the SeeLane vehicle recognition system,

a recognition browser for past and current recognition results.

It displays the recognition results (Vehicle #) and event data (lane#, date/time) and

allows the user to view the images of previous results.

Its inputs are:

a. History results - the recognition log file (log.txt) created by SeeLaneClient application.

b. DDE messages - new events generated by SeeLane/SeeTraffic/SeeRoad LPR systems.

Its outputs are displayed history and images.

It does not save any files, and will discard the collected data when the application is aborted.

2.2.1 It can also be used offline on another PC, if the images directory is set the same name as the original directories.

2.2.2 It can also run on-line on a Central server, assuming that the SeeData tool is used to copy the images across the network.



#### 4.2 Viewing an event

Double click on a event number. It will show the image of that event.

You can also browse with Previous or Next buttons.

SeeLaneClient



The main view displays a list to which items are added for each new data item received from the SeeLane server, all the data will be written to file.

Each row shows another recognition result as reported by the DDE message coming from SeeLane.

The SeeLaneClient can also send 2 kind of triggers to the Seelane by the DDE server message:

- Open Gate trigger.
- Incoming vehicles Trigger.

HELP AND ASSISTANCE;

PLEASE CONTACT Barry T. Dudley on 082 562 8225 or [LPR@I-Cube.co.za](mailto:LPR@I-Cube.co.za)

## 18 Installation Quote

- Bosal conduit, bnc connectors, cabling, labour, (excluding any trenching, electrical work and poles)
- Commissioning and training



### THE MAINTENANCE SERVICE (GOLD)

- a. The provision of corrective maintenance, which means the rendering of services for diagnosing the breakdown of the goods and the subsequent actions necessary to restore the goods to their corrective function.
- b. The provision of preventative maintenance which means the observation of the goods with the intention of identifying minor breakdown or deterioration of the goods and the subsequent actions to restore them to their correct functional and operational state.
- c. Ensuring the continuous and uninterrupted operation of the goods, the repair and maintenance of any faulty goods to the original operational condition and the recalibration and re-commissioning of the affected goods promptly in order to ensure the downtime is kept to an absolute minimum.
- d. The maintenance services include the cost of all parts and consumables, unless such parts or consumables are specifically excluded.

*Should you wish to consider our Silver or Platinum Maintenance plans please feel free to contact me.*





## 19 Equipment Requirement

The performance of the PC and camera equipment is subject to a 220-volt power source at each camera position is to be provided. If required we can arrange an electrician at an additional cost.

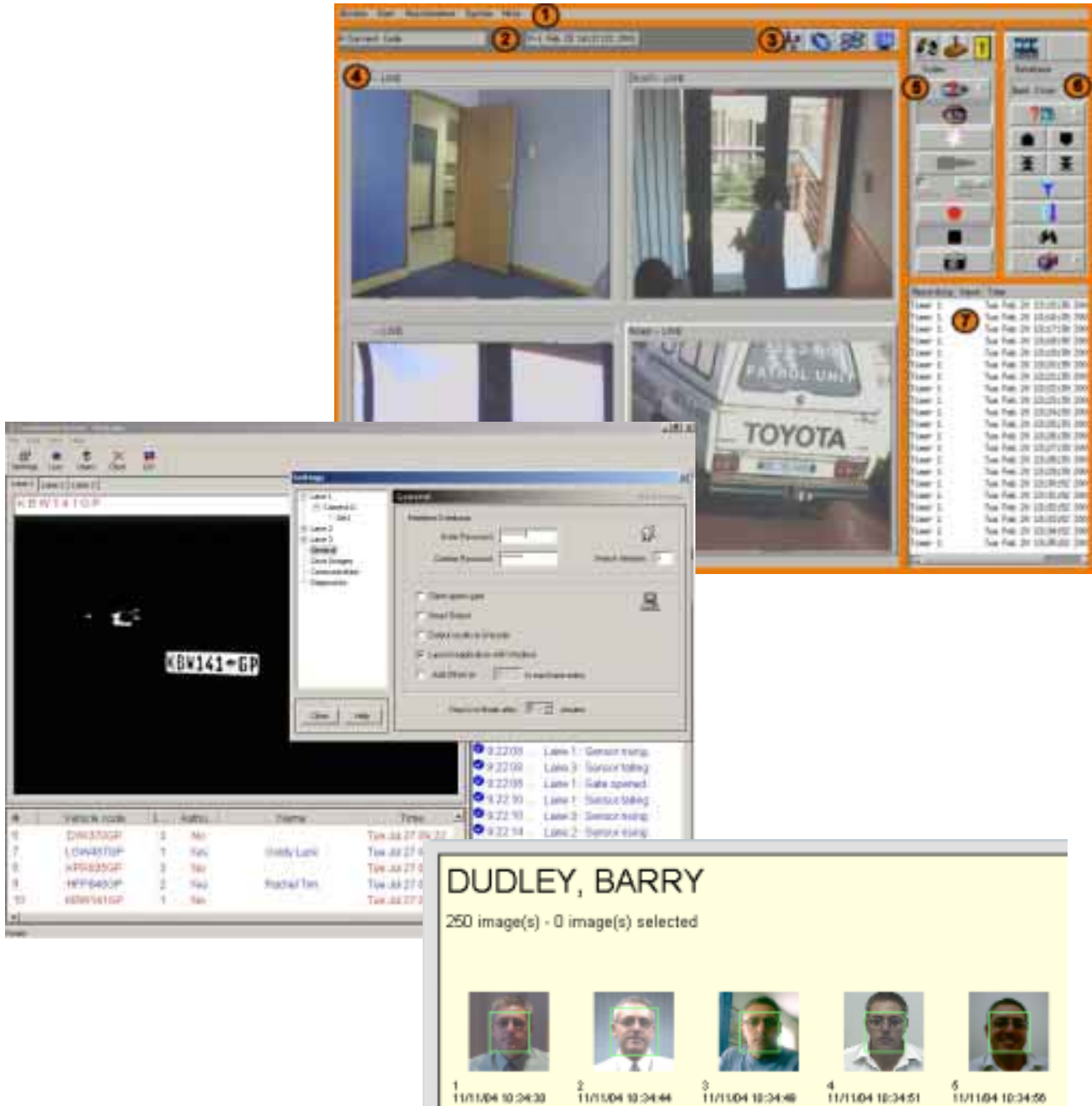
The CCTV signal from the cameras requires fibre to get back to the control room (if more than 75M from the PC).



ESTATE HOME OWNERS ASSOCIATION

## 20 Digital Recorder Integration

Both the LPR and facial identification incorporate into existing DVR systems, allowing the use of existing infrastructure, turning data into information.



# 21 FACIAL IDENTIFICATION SOFTWARE USER MANUAL

## 21.1 How to use I-CUBE Facial Search

### 21.1.1 Enroll

You can enroll face from static image file or live video.

To enroll from static image file, click “Get Photo From File...” button, and select the image file. We currently support JPEG, BMP, WMF and TIFF formats.

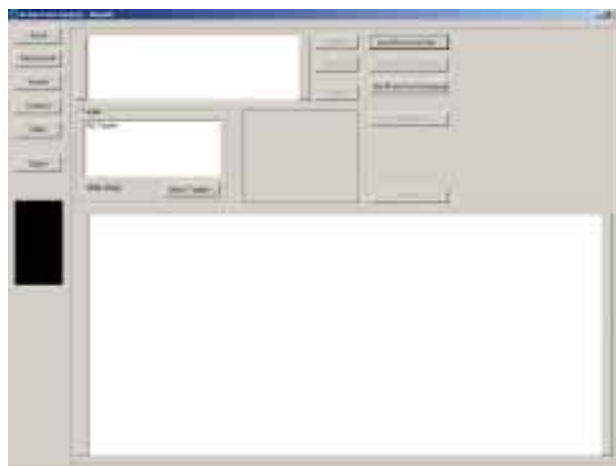
To enroll from vide, you have to enable video if there is no video displayed. You can do it by clicking “Video” button, which is located on left panel. Make sure you have camera and driver installed before doing that. You can adjust the video format and video source by clicking “Video” button again, a dialog box (“Video Settings”) will appear, you can also turn off the video in that dialog box. After video is on, click “Start Track” to start tracking. Click “Get Photo From Video” after face was tracked.

Enter personal information. You have to enter at least First Name and Last Name.

Click “Enroll” button. It will pop up an enrollment successfully message box if everything is fine. Or you may need mark the eyes manually if the system was unable to track the eyes.

### 21.1.2 Batch Enroll

You can do batch enroll to enroll multiple image files.



You have to prepare batch enroll text file. The batch enroll file is a comma or TAB delimited text file. It provides personal information and image file location. For personal information you need have at least First Name and Last Name. Image file location must be file name with full path. So at least you need 3 fields.

For example:  
 Bob, Smith,  
 c:\images\jpeg\1.jpg  
 John, Brown,  
 c:\images\jpeg\2.jpg

You have to enter field ordinates based on your batch enroll file format. According to previous example, we have to put 1 after "First Name", 2 after "Last Name", 3 after "Photo File" and put 0 for all fields you don't use.

Click "..." button to find the batch enroll file, Click "Load" to load the file. You can preview the batch enroll file by "<" and ">" button. By right you should be able to see the photo in that little white box. If not check if the "Photo File" field is correct. Note: we need file name with full path there.

You can still update the field ordinates at this time if you find you entered wrong field ordinates. Just press "Update" button after you updated.

Press "Start" to start batch enrollment if you feel everything is all right. By default it will start enroll from 1<sup>st</sup> record. You can change that by typing number of records to start and click "GoTo" button



before starting batch enrollment.

After batch enrollment is finished, it will give you statistics on number of images enrolled successfully. Some of images you may need mark eyes manually. You can do this by clicking "Mark Eyes..." button. It will go through the database to find out those unmarked images.

Note: those unmarked images are not searchable before you mark them manually.

### 21.1.3 Search

You can search the image from image file, video or database.

To search image from image file, click "Get Photo From File..." button, and select the image file.

To search image from video, enable video, click "Start Track" button and click "Get Photo From Video" after face was tracked.

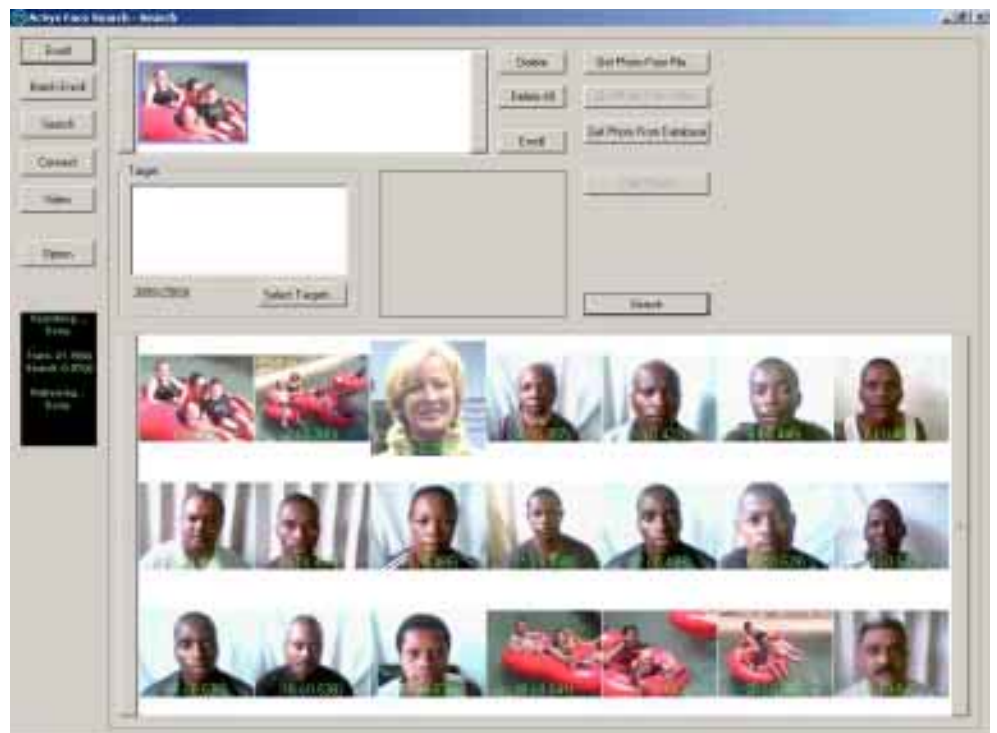
To search image from database, click "Get Photo From Database" button, and select the image in database.

You can search more than one image to get more accurate result. But you must be sure they are the same person.

You can change target data by clicking "Select Targets..." button. By default it will search everyone in database.

Click "Search" button to start search. The result will be showed after search is done.

### 21.1.4 Browse Database



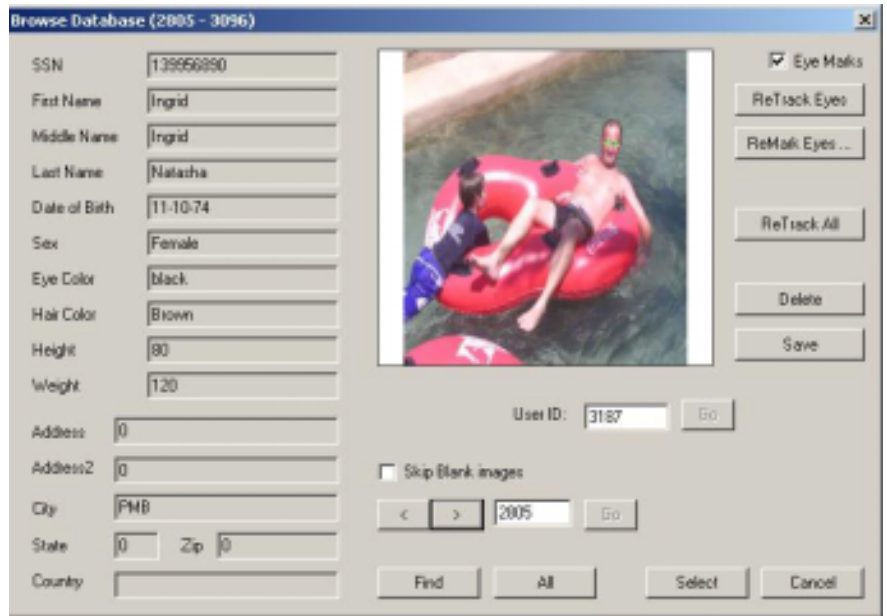
You can do quite a lot of things in browse database dialog box.

You can show eye marks by check "Eye Marks" checkbox.

You can let system re-track eyes for current image by clicking "ReTrack Eyes" button.

You can manually mark the eyes by clicking "ReMark Eyes..." button.

You can re-track all people in database by clicking "ReTrack All" button. Note: you need do this extremely carefully. Coz for big database it may take very long time to finish.



You can delete this record by clicking "Delete" button.

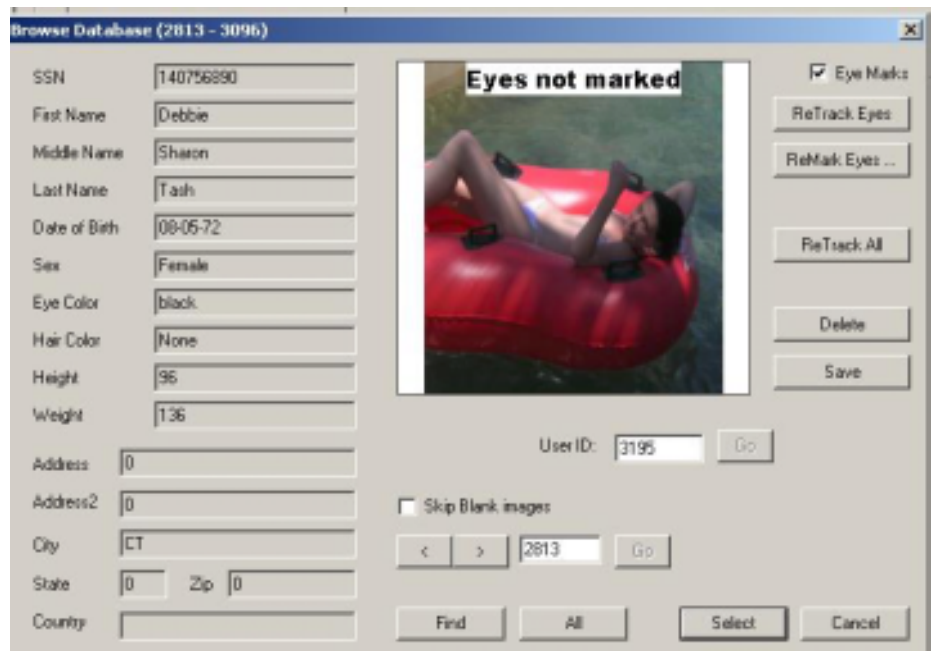
You can save this image to a jpeg file by clicking "Save" button, image will be save as [UserID].jpg.

You can click "Find" button to find the images satisfied with certain condition. After that you can click "All" button to make it back to all dataset.

You can type UserID and click "Go" to go to that record.

You can browse the database by clicking "<" and ">". You can also type number of images to go and go to that record.

"Skip Blank images" means don't display records without image.



## 22 FACIAL VERIFICATION SOFTWARE USER MANUAL

This chapter describes the basic operation of the I-CUBE Discovery system, and how to adjust operational parameters.

Most of the features described in this chapter are common to both Discovery Client and Server-side applications. Features that are available on the Server only are noted.

### 22.1 Basic Operation

The Discovery system (for both standalone and multi-Client installations) provides tracking, verification, and classification functionality. It operates in two views: Standard, and Full-screen.

In Standard view, all functionality is available through menus and buttons, and classification values are graphically displayed. In Full-screen view, the live video display fills the entire screen. Program controls are available through right-click menus.

#### 22.1.1 Connecting to Server

Before running any of the Clients, you must have the Discovery application running on the Server.

When a Discovery Client application is started for the first time, the User is presented with the "Connect" window. A Discovery Client may be connected to any Discovery Server application (i.e. database) currently running on the network.



Figure 2. The Connect window.

- Enter the name of the computer hosting the desired Discovery Server application in the **Server Name** box.
- Click **OK**.

After the Discovery Client is run for the first time, it will not require the Server name again and will connect to the Server automatically. See the [Options](#) section for an explanation of how to connect the Discovery Client to a different Server.

## 22.1.2 Standard View

The main screen of the I-CUBE Discovery is shown below in Standard view.

The Control Buttons on the left side of the screen allow the Operator to run the program in the various modes (i.e. track-only, classify, verify) as well as adjust operational settings and change views.

The Confidence Window in the upper right of the screen provides a display of recognition confidence levels for Classify and Verify operations. This window also functions as a progress bar during enrollment (Add) operations.

Tracking Boxes and Closest Matches are shown in their respective modes.



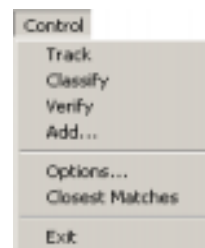
**Figure 3. Discovery Standard view.**

All of the control provided through the buttons are duplicated in the **Control** menu with the exception of the Full-Screen button. Full screen control is provided in the View menu.

Functions provided by the control buttons are described below.

### 22.1.2.1 Track Mode

Click on the **Track** button or select **Track** from the Control menu to enable the facial tracking operation.



While operating in Track mode, the Discovery application will locate any human face within the video frame, place a Tracking Box around the face and follow the face within the frame. The Discovery application is able to track up to 16 faces simultaneously. In Track mode, the application does not attempt to perform identification of the face. Classify and Verify operations must be enabled separately by clicking on buttons located below "Track".

The system will remain in Track mode until the tracking operation is disabled. Click on the **Track** button again to disable facial tracking.

Note that the facial tracking operation cannot be disabled while the Classify or Verify modes are enabled.

### 22.1.2.2 Classify Mode

Click on the **Classify** button or select **Classify** from the Control menu to enable Classify mode (one-to-many identification).





While in Classify mode, the application will attempt to identify tracked faces from the list of users currently enrolled within the system. The results of the classification attempt are displayed in the upper right of the screen in the Confidence Window. When a individual is tracked, and the classification attempt begins, a thumbnail of the tracked face is placed in the upper-right corner of the Confidence Window. Two bars will display the actual confidence values. The bar on the top will display the highest confidence value produced across all users that are currently enrolled. A positive confidence value is shown in green and a negative confidence value in red. The second bar displays the difference between the highest confidence value that is generated for the tracked individual and the second highest confidence value.

The classification threshold is displayed as a tick mark below the confidence display bar. The generated confidence value must exceed this classification threshold while the bar is green, in order for the individual to be classified (i.e. identified). The Confidence Window shown below displays results for up to two tracked individuals.

**Figure 4. The Confidence Window detail.**



If a user is classified (i.e. identified), their name will be displayed on the left of the Confidence Window. If a user is not classified within a timeout period, then “Unknown” will be displayed.

The system can be set up to verbally greet a user on successful classification. See the “Setting Up Speech” section. The system can also automatically register and enroll a user if a pre-set classification timeout period is exceeded. See the “Enrollment” tab description in the “Options Screen” section for setting this timeout period.

Classify mode will continue until it is disabled by again clicking on the **Classify** button. When Classify mode is enabled facial tracking is initiated automatically. After disabling Classify mode, the system will remain in Track mode. Click on the **Track** button to turn off facial tracking.

**22.1.2.3 Show Closest Matches**

Click on the **5-Close** button or select **Closest Matches** from the Control menu to display the 5 closest facial matches from the list of users currently enrolled within the system. The system must currently be operating in Classify mode to enable the display of closest facial matches.

The closest matches are displayed on the right side of the screen and are shown in descending order of recognition confidence.

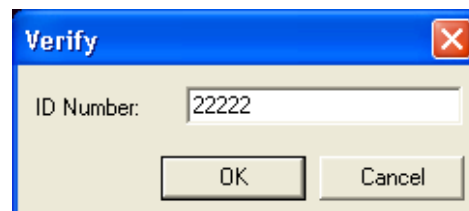


A portrait image of each user within the closest matches list is displayed along with their names and the associated recognition confidence values. Click on the **5-Close** button again to disable display of closest matches. The system will remain in Classify mode.

**22.1.2.4 Verify Mode**



Click on the **Verify** button or select **Verify** from the Control menu to enable the verify operation (one-to-one identification).



After clicking the Verify button, the Verify window will appear.

Enter the users ID number in the Verify window and click **OK**. The verification operation will then commence. The user will be tracked and compared against the corresponding user that has been previously enrolled by the system.

The recognition confidence value of the comparison will be displayed in the Confidence Window. If this confidence value exceeds the verification threshold, the user will be verified and any corresponding actions that have been preset during program setup will be executed (i.e. relay contact activation, NetAlert alarm, Wiegand signal pass-through).

The Verification Threshold may be modified within the Options window.

When in Verify mode, the tracking operation is enabled automatically. Click on the **Verify** button to disable the verify operation, facial tracking will remain active. Click on the **Track** button to disable the tracking operation.

Extensions have been provided which combine the verify operation with a Keyscan Wiegand Serial Interface and a NCD Relay (model R42, R410, or R810).

The Wiegand Serial Interface can be connected to various Promixity or Wiegand card systems to provide ID card or keypad based functionality. If a card reader or keypad system has been set up, the system will automatically begin verification on either keypad entry or card swipe.

If a relay system has been set up, the system can close or open an external circuit, such as a door strike, on verification (or classification).

See the “Extensions” section for more details regarding peripheral devices such as relays and Wiegand devices.

### 22.1.2.5 Add New User

Click on the **Add** button or select **Add** from the Control menu to add a new user to the system and start the enrollment process.



When the **Add** button is clicked, the “Enter Name” window will appear..

**Figure 5. The Enter Name window of the Add User function.**



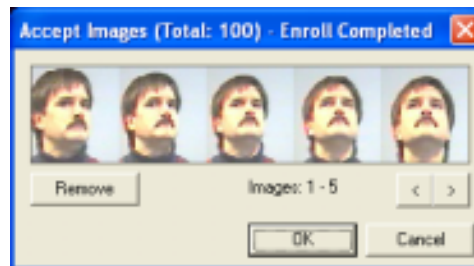
- Enter the User’s first name in the **First Name** box.
- Enter the User’s last name in the **Last Name** box.
- Enter the User’s card number in the **ID Number** box.
- Enter the number of images you wish to collect of the User in the **Number of Images** box. 100 is the default value.
- Click **OK**.



The enrollment process will begin whereby facial images of the user are collected and subsequently added to the FRS database. The enrollment progress is shown within the Confidence Window. A green progress bar will move further to the right with each image that is collected.

When the number of images specified in the “Number of Images” box have been collected, the enrollment operation will terminate. If the system times out prior to capture of the specified number images, or the user leaves the cameras frame for a period of time (default 20 seconds), the enrollment operation will fail. The default value for the timeout condition can be modified in the Enrollment options (Section 3.2.3).

When the enrollment operation has finished, the user will be asked to accept the enrolled images. The Accept Images window provides the operator the option to remove facial images of poor quality or images of people who may have been incorrectly tracked during the enrollment operation.

**Figure 6. Accept Images window is shown at the end of enroll.**



The operator may scroll through the collected images using the  and  buttons. Single images may be removed by selecting the image and clicking the **Remove** button.

If the operator is satisfied with the enrolled images, click the **OK** button to accept images and allow the system to begin generating the biometric template for that user.

The system will collect images faster if the user being enrolled provides different expressions, at different head angles, lighting conditions and at varying distances from the camera. It is normal for users new to the system to stare fixedly at the video display. To achieve optimal performance, you must create a situation in which the user is moving their head and walking to create varying lighting conditions. The operator should instruct the user to move naturally and/or walk towards the camera.

The system may also be set to issue verbal commands to the user in order to Guide the enroll procedure (see the “Setting Up Speech” section at the end of this chapter).

**22.1.2.6 Show Options**

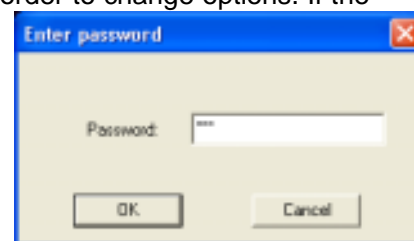
Click the **Options** button or select **Options** from the Control menu to display the Options window.



The Options window allows the user to modify operational settings within the Discovery system. See the “Options” section for a detailed description of the Discovery system options.

The I-CUBE Discovery may be setup to require a password in order to change options. If the password option is set the following window will appear when clicking the **Options** button. Enter the Options password and click **OK**.

**Figure 7. Password dialog.**



The Options password protection is enabled and disabled in the General tab of the Options window.

### 22.1.2.7 Full-Screen View

Click the **Full-Screen** button or select Full-Screen from the View menu to switch Discovery to Full-Screen view.



In Full-Screen view, the video window expands to fill the entire display. All controls shown in Standard view will be hidden. A subset of the controls are available in Full-Screen view through a right-click popup menu. See the Full-Screen View section later in this chapter for details.

### 22.1.2.8 Exit

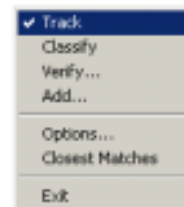
The Exit button is located at the bottom right of the Discovery application when in Standard view.



This button closes the application. Note that closing the Client application on the Server machine does not stop the Server application. For information on terminating the Server Application refer to [Chapter 4](#).

## 22.1.3 Full Screen View

By switching to Full-Screen view, the video window will expand to fill the entire display area. All menus and controls will be hidden.



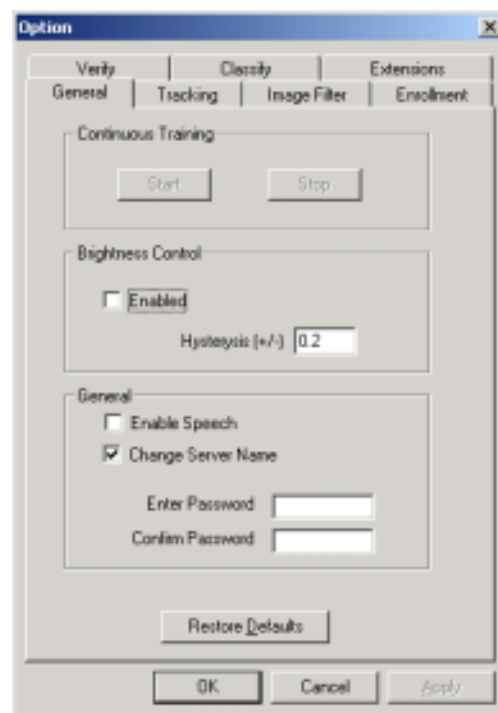
In Full-Screen view, the user has control over a subset of the Standard view's operational features. These operational features include:

- Track Mode
- Classify Mode
- Verify Mode
- Add New User
- Show Closest Matches
- Show Options
- Exiting the Application

Database editing and display features are not available in the Full-Screen view.

To exercise the features in Full-Screen view, right-click anywhere on the screen. A popup menu will appear. Select the desired feature from the popup menu.

**Figure 8. Popup menu for full screen mode.**



To return to Full-Screen view, press the **ESCAPE** key.

While in Full-Screen view, Closest Matches mode will display the closest matches on the right side of the screen.

## 22.2 Setting Operating Parameters

The options form allows the User to adjust various operating parameters of the Discovery system. This form is enabled by clicking the **Options** button outlined in the previous section. The options form is divided into eight tabbed sections.

### 22.2.1 General Tab

The tab shown below allows the operator to adjust options that pertain to continuous re-generation (training) of the biometric templates used during classify and verify operations, options for automatic brightness compensation, enabling speech synthesis, password protection on program variables, changing the Discovery Server and resetting parameters to default values.

**Figure 9. Options window - General tab.**

#### 22.2.1.1 Continuous Training Panel

The Continuous Training option is available on the Discovery Server application only. When this option is enabled, re-generation of all biometric templates within the Discovery Server database is performed continuously in order to improve the speed and accuracy of verification and classification operations.

Continuous training is performed by the FRS Training Server while it is running. By default, the continuous training operation starts automatically on startup of the Server. To stop continuous training click the **Stop** button.

Note that training can be controlled directly through the FRS Training Server, for further details refer to Chapter 4.

#### 22.2.1.2 Brightness Control Panel

Brightness control adjusts the video capture driver to compensate for mean pixel intensity located within the region of the tracked face. Hysteresis is applied to brightness control and limits the amount of compensation applied.

#### 22.2.1.3 General Panel

The facilities provided within the Common panel allow the operator to enable or disable synthesized speech, reconnect to a different Discovery Server and provide password protection for program option settings.

##### 22.2.1.3.1 Enable Speech

By default, synthesized speech within the Discovery Client application is not enabled. To activate speech, check the **Enable Speech** box. Click **OK** and restart the Discovery application. Speech synthesis will now be enabled for all operations such as enroll, classification, and verification.

See the "Setting Up Speech" section later in this chapter for details on customizing speech.

##### 22.2.1.3.2 Change Server Name

This control is enabled only for Discovery Client machines. If this control is checked, the Discovery system will request the Server name on the next start up of the application. This feature allows the user to connect the Discovery Client to a different Server within the network.

### 22.2.1.3.3 New Password

The operator may enable password protection for the setting of options and pushbutton configurations. Password protection is disabled by default. Entering characters within this text box and confirming text box enables password protection. Password protection may be disabled by clearing the password and confirming text box.

### 22.2.1.4 Restore Defaults

If the system begins to behave erratically, option settings may have been changed to an unserviceable combination. Click the **Restore Defaults** button to restore all settings to their default installation values. This button effects the settings defined within all tabs, including the General tab.

## 22.2.2 Enrollment Tab

The tabbed section entitled "Enrollment" allows the User to adjust parameters that control the enrollment operation. Note that the option is provided to perform enrollment following a successful verification. This allows the system to update the template continuously during normal usage.

**Figure 10. Options window - Enrollment tab.**

Descriptions of the various parameters that may be adjusted for enrollment operations are as follows:



### 22.2.2.1 Parameters Panel

The facilities provided within the Parameters panel allow the operator to set capture frame intervals, thresholds for pattern variance on image capture and enrollment timeouts.



#### 22.2.2.1.1 Frame Interval

During an enrollment operation the system collects an image from every  $n^{\text{th}}$  video frame that is captured. This helps to ensure a greater variation across the set of enrolled images. This parameter sets the image frame interval for image capture.

#### 22.2.2.1.2 Image Difference Threshold

Each image that is captured for enrollment must be sufficiently different from the previous enrollment image, in order to ensure reasonable variation among the images collected during enrollment. This value sets the variance (pattern difference) threshold which must be within the range 0.0 to 1.0.

#### 22.2.2.1.3 Track Timeout

The enrollment operation will terminate automatically if the system is unable to track the user for a period of time (in seconds) specified by this setting.

### 22.2.2.2 Verification Panel

The facilities provided within the Verification panel allow the operator to set parameters concerning automated re-enrollment performed following a successful verification operation.

#### 22.2.2.2.1 Enable Enrollment During Verify

When this flag is checked, Discovery will enroll a preset number of facial images during each successful verify operation. This allows the system to continually adapt and refine the biometric template over time.

#### 22.2.2.2.2 Maximum Images

This value determines the maximum number of additional facial images that Discovery will enroll during each successful verification operation.

#### 22.2.2.2.3 Confidence Threshold

Images collected for enrollment during verification must have a confidence value less than this threshold. This ensures that only images containing a new perspective view of the user will be enrolled.

#### 22.2.2.3 Enroll During Classify

If this control is checked and a classification operation exceeds the timeout duration (default 6 seconds), the system will present the "Enter Name" dialog and enroll a new user. For information on classification timeout refer to the section describing the classify options. If this box is not checked, users will not be enrolled following a classify timeout condition and the system will speak a pre-set phrase (i.e. Could you please register with the receptionist, thank you.).

#### 22.2.2.4 Enroll Pre-Registered Only

If this box is checked, the system will automatically enroll a user who has been pre-registered the first time they perform a verification operation via the "Wiegand" interface. While this option is enabled the **Add** button is removed.

### 22.2.3 Tracking Tab

The tabbed section entitled 'Tracking' allows the operator to adjust parameters concerning facial tracking. These parameters apply to all modes of operation, which include "Tracking", "Enrollment", "Classify" and "Verify". The tracking subsystem is based upon a "Knowbot" structure, consisting of a geometrical arrangement of retinal viewing areas. This knowbot structure performs a scan over the video capture frame looking for peaks in the recognition topology. The neural assembly forming the "brains" behind the retina has been trained to recognize human faces. The system also uses basic cues to estimate where a face may be located. These cues are based upon image variance, movement, and color. The options dialog for the tracking parameters are shown below:

Figure 11. Options window - Tracking tab.



A description of the various parameters that may be adjusted for the facial tracking operation are described as follows:

### **22.2.3.1 Parameters Panel**

The facilities provided within the Parameters panel allow the operator to set tracking sensitivity and the range of facial sizes for tracking operations.

#### **22.2.3.1.1 Follow Threshold**

Determines the confidence threshold associated with the knowbot structure for determining whether the segmented region corresponds to a face. If the confidence remains above this threshold, the knowbot will continue to follow the face on subsequent video frames.

#### **22.2.3.1.2 Maximum Size**

This text box sets the upper size limit for faces that are tracked. This size limit is applied for tracking during all modes of operation (i.e. enrollment, classify and verify ). The size of the facial tracking box is established as a fraction of the height of the video frame.

#### **22.2.3.1.3 Minimum Size**

This text box sets the lower size limit for faces that are tracked. This size limit is applied for tracking during all modes of operation (i.e. enrollment, classify and verify ). The size of the facial tracking box is established as a fraction of the height of the video frame.

### **22.2.3.2 Mask Thresholds Panel**

The panel entitled "Mask Thresholds" panel pertains to a series of masks that are applied over the video frame, sectioned into 16 x 16 regions. Each region of the video frame is evaluated separately for variance, frame to frame movement and color content. Thresholds are applied to these measurements in order to mask out regions of the video frame from the tracking subsystem. Proper use of masks can significantly improve tracking speed and performance. It should also be noted that the effect of the masks may be viewed by clicking on the "View/Show Masks/All" menu items. Descriptions of the parameters contained within the "Mask Thresholds" panel are provided below:

#### **22.2.3.2.1 Variance**

The variance measurement within each region is normalized by variance across the entire video frame. This set point is used when the variation over time in overall lighting intensity is large. If relative pixel intensity variance is less than this threshold, the region will be masked out.

#### **22.2.3.2.2 Abs Variance**

Similar to the "Variance" threshold, however the threshold for masking out regions of the video frame based upon an absolute measure of pixel intensity variance. If intensity variance is less than this threshold, the region will be masked out.

#### **22.2.3.2.3 Movement**

Sets a difference threshold for frame-to-frame pixel intensity. This value is used to detect motion. If the frame-to-frame difference in pixel intensity is less than this threshold, the region will be masked out.

#### **22.2.3.2.4 Face Color**

Regions of the image may be masked out based upon color content. This value sets the mask threshold for skin tone. The color scoring method has been tuned to recognize skin tone among all ethnic types. The valid range for this parameter is -1 to +1. Lower values will cause a greater region of the video frame to be masked out.



### 22.2.3.2.5 *Advanced*

The above masks may be applied in various combinations using an 8 frame cyclical schedule. This schedule may be modified by clicking on the "Advanced" pushbutton which enables the following screen:

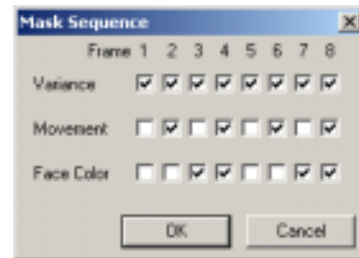


Figure 12. Tracking Masks dialog.

The masking conditions that are checked along each column are combined using a logical OR relationship.

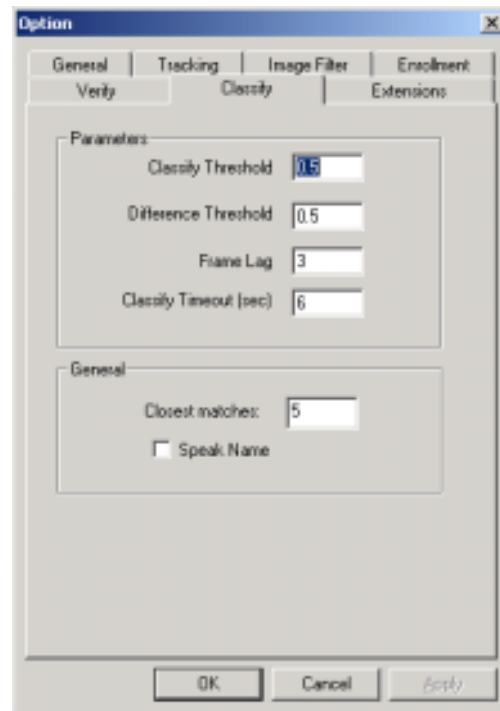
## 22.2.4 **Classify Tab**

These settings affect the classification (one-to-many identification) operation. The option is provided to set recognition thresholds, confidence lag factor and the classification timeout value.

Figure 13. Options window - Classify tab.

### Parameters Panel

Descriptions of the various parameters that may be adjusted for the classify operation are as follows:



#### 22.2.4.1.1 *Threshold*

The output value (recognition confidence) generated by biometric templates range from -1 to +1, with +1 indicating high confidence in recognition. This threshold establishes the set-point above which an individual is positively identified (i.e. classified). This threshold is applied in conjunction with the difference threshold described below.

#### 22.2.4.1.2 *Difference Threshold*

This threshold pertains to the difference between the highest confidence value that is generated among all individuals that are enrolled within the system, and the second highest confidence value. This difference must be greater than the specified threshold in order for the system to register a positive identification.

#### 22.2.4.1.3 *Frame Lag*

The recognition confidence values that are generated across all biometric templates are lagged by video frame count. This value establishes the degree of digital lag that is applied to the recognition confidence values when the system is operating in classify mode.

#### 22.2.4.1.4 *Classification Timeout*

This value specifies a timeout condition that is applied to the classification operation. In the event that the user is not recognized within the specified time period, the system will either perform an automated enrollment operation or produce synthesized speech from a pre-set

text string (i.e. Could you please register with the receptionist, thank you.). The option for selecting either automated enrollment or speech response is provided within the Enrollment tab.

**22.2.4.2 General Panel**

The general panel allows the operator to set the number of closest matches displayed during classification operations and disable or enable speech synthesis for speaking the users name.

**22.2.4.2.1 Closest Matches**

This number determines the number of people that will be displayed on the right side of the screen when the Closest Match display is enabled. The maximum number of closest matches displayed is five.

**22.2.4.2.2 Speak Name**

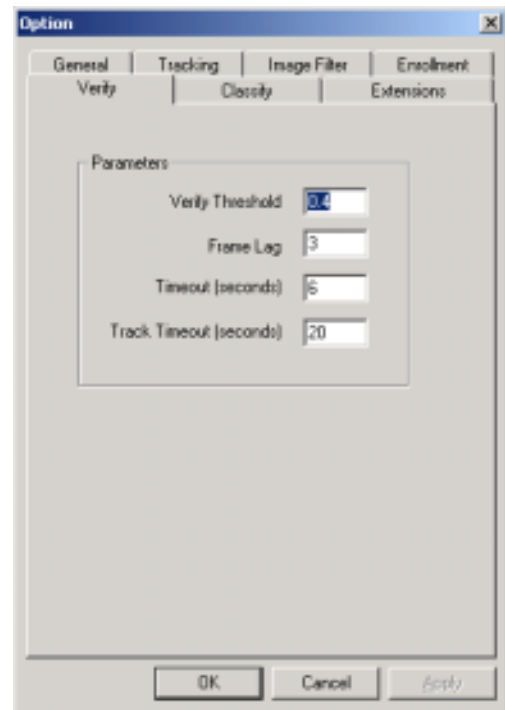
If this box is checked the system will speak the individuals name in addition to a preset speech string, following a successful classification. If unchecked, only the speech string (without name appended) will be generated.

By default all synthesized speech is deactivated and must be enabled in order for this option to be enabled. Refer to the description of the "General" tab for details on activating speech.

**22.2.5 Verify Tab**

These settings affect the verification (one-to-one identification) operation. The option is provided to set recognition thresholds, confidence lag factor, head orientation boundaries and the distance range applied during Verification.

**Figure 14. Options window - Verify tab**



**22.2.5.1 Parameters Panel**

A descriptions of the various parameters that may be adjusted for the verify operation are as follows:

**22.2.5.1.1 Threshold**

The output value (recognition confidence) generated by biometric templates range from -1 to +1, with +1 indicating high confidence in recognition. This threshold establishes the set-point above which an individual is positively identified.

**22.2.5.1.2 Frame Lag**

The confidence values generated across all biometric templates are lagged by the video capture frame count. This value establishes the degree of digital lag applied to the recognition confidence values when the system is operating in verify mode.

### 22.2.5.1.3 Timeout (seconds)

Sets the maximum number of seconds provided for the verify operation. The corresponding timer is incremented only while tracking is active. In the event that the individual is not verified within this cumulative time interval, the system registers a verify failure and generates the pre-set response (i.e. synthesized speech).

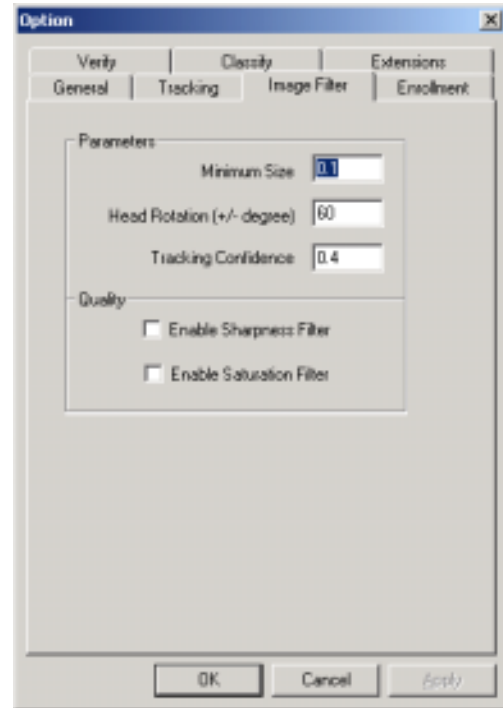
### 22.2.5.1.4 Track Timeout (seconds)

Sets an absolute timeout period for the verify operation regardless of whether tracking is active (i.e. timeout condition in the event that the user walks away from the camera prior to being verified). If the system is unable to verify the face in less than the specified interval (default 20 seconds) a failed verify attempt is recorded.

## 22.2.6 Image Filter Tab

Facial images captured during enrollment, verification or classification operations may be filtered in order to improve the quality of training data and improve recognition accuracy.

Figure 15. Options window - Image Filter tab.



### 22.2.6.1 Parameters Panel

The facilities provided within the Parameters panel allow the operator to set the conditions which filter out images for all enrollment, verification and classification operations. These parameters concern minimum head size, head rotation limits and minimum tracking confidence values. Also provided are filters for image quality concerning image sharpness and saturation.

#### 22.2.6.1.1 Minimum Size

This text box sets the lower limit with respect to the size of the face that is used for enrollment, verification and classification operations. The size of the tracking box is established as a fraction of the height of the video display. In the event that the tracked facial image is smaller than the specified size, a verbal command is issued asking the individual to move closer to the camera. The valid range for this parameter is 0.05 to 1.0. In the figure above, only faces larger than 1/10 the screen height are processed during enrollment, verification or classification operations.

#### 22.2.6.1.2 Head Rotation (degrees)

Establishes the permitted range in head rotation for facial images that are used for enrollment, verification and classification operations. In the event that the head is rotated away from the camera by an angle greater than that specified, those images will not be used in any of the above operations. In the figure above, only images with head orientations less than 60 degrees from full frontal are processed during enrollment, verification or classification operations.

#### 22.2.6.1.3 Tracking Confidence

While the system is performing tracking, a confidence value is generated in terms of how closely that image resembles a human face. Tracked images that generate a confidence less

than this setting will not be processed during enrollment, verification or classification operations.

**22.2.6.1.4 Sharpness Filter**

Poorly focused images are rejected by checking this box.

**22.2.6.1.5 Saturation Filter**

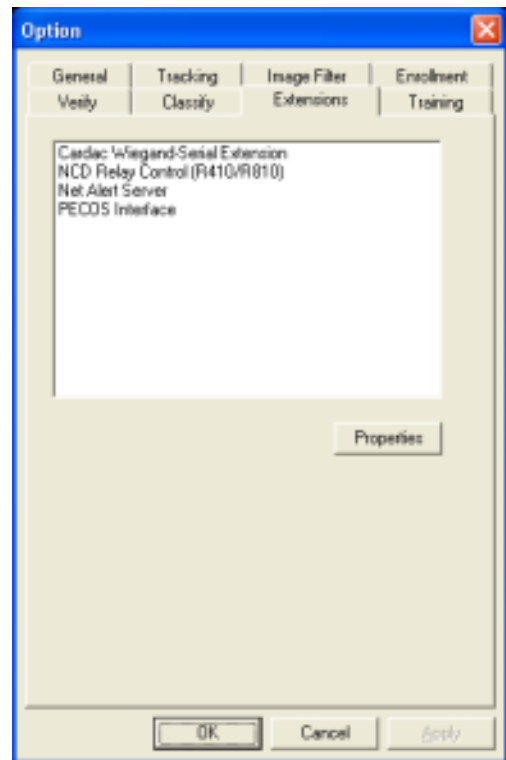
Facial images that are either overexposed or underexposed are rejected by checking this box.

**22.2.7 Extensions**

Extensions are plug-ins to the system that provide extra functionality by reacting to events and interfacing to peripheral devices. Extensions provided with the Discovery System provide peripheral control for Wiegand interfaces, dry contact relay outputs, and mobile (wireless) computing devices.

The ‘Extensions’ tab shown below modifies properties associated with these program extensions.

**Figure 16. Options window - Extensions tab.**



Operational parameters concerning an extension are adjusted by highlighting the extension name on the above form and clicking the **Properties** button. The operational features/characteristics provided by each extension are described below.

**22.2.7.1 NCD Relay Control (R410/R810)**

This extension provides logic to toggle dry contact relay outputs on the following events:

- verify success
- verify failure
- classification success
- facial tracking
- ID card or keypad usage (through Wiegand interface)

Selecting the “Properties” option for the relay extension enables the following form:

**Figure 17. Relay Options dialog.**



Relay contacts are selected by enabling the checkbox located on the left side of the screen. The operation that controls the relay (i.e. verify, classify, track or Wiegand signal) is selected using the option buttons located on the right side of the screen. The duration that the relay

remains activated is adjusted by entering an integer value into the textbox located to the right of the relay contact selection checkbox.

### 22.2.7.2 Cardac Wiegand Serial

The Cardac Wiegand Serial extension provides an interface for any Wiegand input device, typically a magnetic ID card or keypad.

On swipe of an ID card, or input from any compatible Wiegand device, the system will initiate a verify operation. If the user has been registered but not enrolled, the system will automatically initiate the enrollment procedure. See the “Enrollment” Options for details.

To set the options for the Wiegand Extension, select **Cardac Wiegand Serial Extension** from the Extensions list, and click **Properties**. The Options dialog will appear.

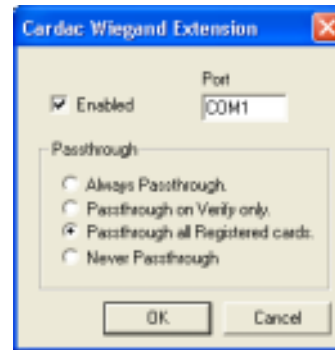


Figure 18. Cardac Wiegand Extension dialog.

#### 22.2.7.2.1 Enabled

Enables the Extension if checked. Disables the Extension if not checked.

#### 22.2.7.2.2 Port

Specifies the COM port connected to Wiegand Serial Interface device.

#### 22.2.7.2.3 Passthrough

In all cases, when a Wiegand device is activated (through card swipe or keypad entry) and the user associated with the ID number is both registered and enrolled within the system, a verification operation is initiated.

##### 22.2.7.2.3.1 Always Passthrough

The ID number is passed through the system to be received by an external Wiegand device regardless of whether verification is successful or not. The external Wiegand device is generally a legacy door access control system.

##### 22.2.7.2.3.2 Passthrough on Verify Only

The ID number will only be passed through if the user has been verified.

##### 22.2.7.2.3.3 Passthrough all Registered Cards

*22.2.7.2.3.4 The ID number is immediately passed through regardless of whether verification is successful or not, however only registered ID numbers will be propagated.*

##### 22.2.7.2.3.5 Never Passthrough

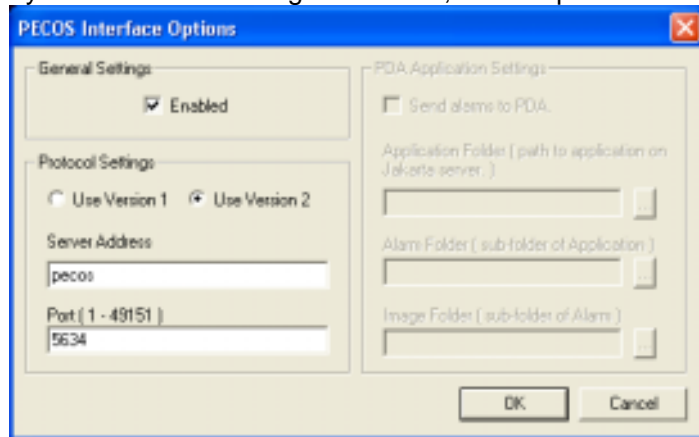
The ID number will not be passed through regardless of whether verification is successful or not.

### 22.2.7.3 PECOS Interface

The PECOS Interface extension allows the Discovery System to send alarms to the PECOS system, and to wireless Pocket PC devices that interface directly to the PECOS system.

The PECOS protocol is a TCP-based message that allows external systems to send alarms and alarm information to the PECOS system. Each message is atomic, and requires no reply from the PECOS system. Messages are 7-bit ASCII text and require no handshake.

There are two versions of the PECOS protocol. Each version defines a READY message and a MATCH message. Version 1 is extended to include Pocket PC support. The dialog for configuring the PECOS interface is shown below:



**Figure 19. PECOS Interface Options dialog.**

### **22.2.7.3.1 General Settings**

#### **22.2.7.3.1.1 Enabled Checkbox**

When this checkbox is enabled, the extension will send messages to the computer (PECOS server) specified by *Server Address* and *Port*, using the version protocol specified in the Protocol Settings.

### **22.2.7.3.2 Protocol Settings**

#### **22.2.7.3.2.1 Use Version 1**

When this option is selected, both READY and MATCH messages will be sent to the machine specified by *Server Address* and *Port*. “PDA Application Settings” are only available with Version 1.

#### **22.2.7.3.2.2 Use Version 2**

When this option is selected, pseudo-XML messages will be sent to the machine specified by *Server Address* and *Port*. These messages will contain detailed information regarding User, Location, Time, and alarm type. A snapshot is also embedded in the Version 2 message. PDA Application Settings are not available with Version 2.

#### **22.2.7.3.2.3 Server Address**

IP Address or UPC name of the machine to which all messages will be sent. This should be the machine on which the PECOS server resides. If a UPC name is used, it must be registered with your network’s DNS. IP Addresses are generally more reliable.

#### **22.2.7.3.2.4 Port**

Port on the machine that will receive messages. The Port number must match between PECOS system server and this extension. All external systems connect to PECOS on the same Port. Valid port numbers range from 1 to 49151.

### **22.2.7.3.3 Pocket PC Application Settings**

### 22.2.7.3.3.1 Send Alarms to Pocket PC

When this flag is set, and Version 1 has been selected, and the extension is enabled, the extension will send messages to the PECOS Pocket PC system on classification.

### 22.2.7.3.3.2 Application Folder

Path to the Pocket PC application on the Jakarta server that hosts the PECOS web application. This value can only be set if the *Send Alarms to PDA* flag is checked. The path is chosen by clicking the browse button to the right of the field.

### 22.2.7.3.3.3 Alarm Folder

Alarm sub-folder of the PDA Application Folder for the PECOS web application. This folder will receive all XML files generated by the PECOS extension. This value cannot be set until the *Application Folder* is set. The folder is chosen by clicking the browse button to the right of the field.

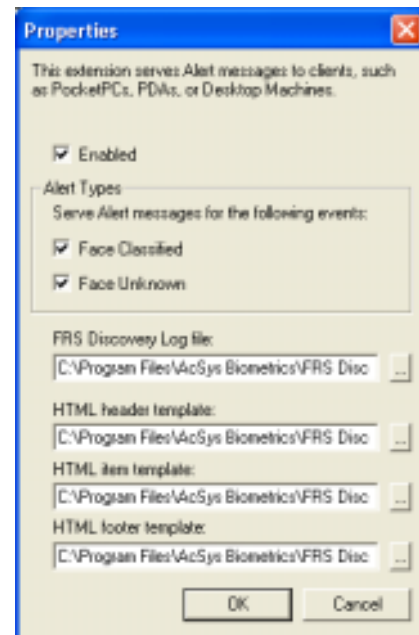
### 22.2.7.3.3.4 Image Folder

Image sub-folder of the *Alarm Folder* for the PECOS web application. This folder will receive all JPEG files generated by the PECOS extension. This value cannot be set until *Alarm Folder* is selected. This folder is selected by clicking the browse button to the right of the field.

### 22.2.7.4 NetAlert Server

This extension enables a Pocket PC equipped with wireless communication to receive HTML alarm messages and JPEG images from the Discovery System. The dialog for configuring the NetAlert Server that provides messages to the Pocket PC is shown below:

Figure 20. NetAlert Properties dialog.



The following check boxes are used to enable messages to the Pocket PC.

#### 22.2.7.4.1 Enabled

Enables and disables the notification of security alerts. The Discovery System will only send messages to the Pocket PC when this box is checked.

#### 22.2.7.4.2 Face Classified.

Sends an alarm to the Pocket PC when a user is successfully classified (one-to-many identification).

#### 22.2.7.4.3 Face Unknown

Send an alarm to the Pocket PC when a classification operation times out.

The following filenames must be entered into the text boxes in the lower section of dialog in order for the system to function.

#### 22.2.7.4.4 Path to FRS Surveillance Log file

The NetAlert Server receives its information from the FRS Discovery log. Set the path to the log file here. **This path must be set before NetAlert will function!**

#### 22.2.7.4.5 HTML Template Files

The alarm messages are sent to the Pocket PC in HTML format. Templates have been used to allow the user to change the appearance of the HTML page. The entry templates are stored as UTF-8 text. The default installation will place these files in folder c:\andface. The following three templates are used to generate each HTML page and either the pre-configured or modified templates must be assigned.

#### 22.2.7.4.6 HTML header template

The HTML source code that precedes the alert information. Any header or meta information normally goes here. The filename for the header template is header.txt

#### 22.2.7.4.7 HTML item template

Used to display the HTML code for each alert. The filename for the item template is entry\_template.txt

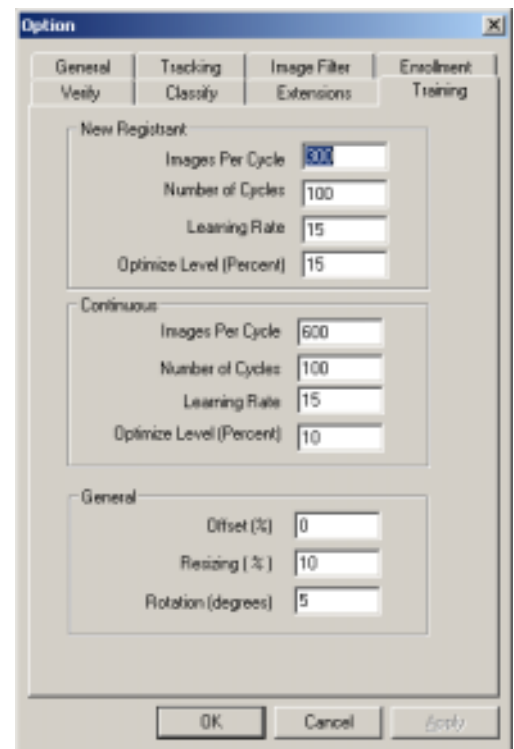
#### 22.2.7.4.8 HTML footer template

The HTML code that follows the alert items. The filename for the footer template is footer.txt

### Training

Training options are only available on the Discovery Server application. They are accessed through the Training tab within the Options screen. These training parameters effect the generation of biometric templates, performed after facial images have been collected during an enrollment operation.

Figure 21. Options window - Training tab.



#### 22.2.7.5 New Registrant

The top panel entitled "New Registrant" adjusts parameters regarding the generation of biometric templates (i.e. training) performed immediately after a user has been enrolled. These training parameters are also applied when re-generating the biometric templates across all enrolled users, initiated by clicking the "Database/Reset Database" menu items. The first text box sets the number of images used within each training cycle, and the second text box adjusts the number of training cycles. The third text box entitled "Learning Rate" sets the learning rate that is applied during the generation of templates. The learning rate should be set within the range 5% to 40%. The last text box sets an optimization level that is applied, this value should also be set within the range 5% to 40%.

#### 22.2.7.6 Continuous

The lower panel entitled "Continuous" adjusts the same training parameters as those indicated above. These settings are applied when performing the continuous training operation, which updates biometric templates continuously using a background processing thread.



### 22.2.7.7 Image Parameters

Prior to generation of the biometric template (i.e. training), the system will manipulate enrolled facial images in order to provide a more robust set of training images. This process randomly offsets, resizes and rotates the enrolled images. The Image Parameters determine the upper limits applied to manipulation of training images.

#### 22.2.7.7.1 Offset

The maximum amount of offset applied to facial images over both the horizontal and vertical axis. This is specified as a percentage of the image size.

#### 22.2.7.7.2 Resize

The maximum degree of resizing applied to facial images. This is specified as a percentage of the original image size.

#### 22.2.7.7.3 Rotation

The maximum amount of rotation applied to facial images, specified in degrees.

## 22.3 Server Database

The database of facial images may be viewed and edited only from the Discovery Server machine. The operational features provided under the database menu item are:

- Viewing and deletion of images stored within the FRS database and applied during biometric template generation
- Clearing and regeneration of all biometric templates stored within the database
- Batch pre-registration of users from an ASCII text file
- Enrollment of users from static (JPEG) images

### 22.3.1 Editing the Database

The “Edit Database” utility allows the operator to view and delete images stored within the Discovery Server database and used in generation of biometric templates. To enable this screen select **Edit Database** from the *Database* menu.



Figure 22. Edit Database window.

From the Edit Database screen, the operator may remove any subset or all training images for the selected user. The set of registered users is shown in the list box located on left side of the screen. Users are listed by [lastname, firstname] and ID number.

The name of the currently selected user is shown in the **Select User** box. The facial images that are stored for the currently selected user are shown in the right panel.

The list of enrolled users may be sorted by clicking on the Name or Card column header. Clicking on the Name column header will sort the users alphabetically by name in ascending or descending order. Clicking on the Card column header will sort the list by Card number in ascending or descending order.

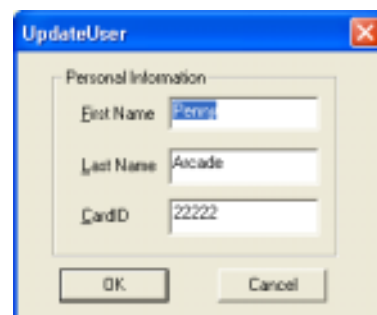
To select a different user for display and editing, click the associated name in the list box, or enter a name in the **Select User** box and press ENTER. Users may be searched by Name or Card number.

To search for a specific user by Name, click on the **Name** column header to pre-sort the list, then enter the users last name or the beginning letters of the last name in the Select User box, and press **ENTER**.

To search for a specific user by Card, click on the **Card** column header to pre-sort the list, then enter the user's card number or the beginning digits of the card number in the Select User box, and press **ENTER**.

To edit the users information, double-click on the user name in the list box. The following Update User dialog will appear.

**Figure 23. Update User dialog.**



In the Update User dialog, you may change the first name, last name, and card number.

To delete a user, right-click on the users name in the list box and select **Delete**. Multi-select may also be applied when deleting users.

To delete an image, select by clicking on the image and a blue boarder will appear. Click the **Remove** button. The image will be removed from the system and is no longer applied during template generation.

You may multi-select images for removal by clicking on the first image you wish to remove, then hold down the SHIFT key and click on the last image within the image set. All the images between the first and last images will be selected. Click on the **Remove** button to remove the selected images.

Click the **Remove all** button to remove all training images for the currently selected user.

### 22.3.2 Exporting Users

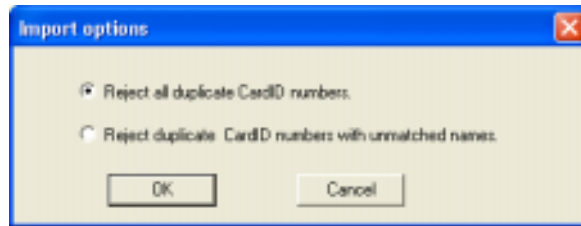
Users may be exported from the Discovery database for subsequent import into a separate Discovery installation. To export a user or multiple users, select the user(s) within the list box, right-click and select **Export Users**. A common file dialog will appear. Enter the name of the file that is to contain the exported data and click **Save**. All data including training images, will be exported to the file.

### 22.3.3 Importing Users

Users may be imported to the Discovery system from a previously saved export file. Select **Import Users** from the **Tools** menu and choose the file to be imported. The Discovery application will create a new user within the Server database for each user stored within the export file.

### 22.3.3.1 Import Options

During import of users, it is possible that the export file contains one or more user ID numbers that already exist within the current Discovery database. To deal with possible duplication of user IDs during import, the Import Options dialog provides two methods. To access the Import Options dialog, select **Import Options** from the *File* menu.



**Figure 24. The Import Options dialog.**

#### 22.3.3.1.1 Reject all duplicate CardID numbers

If this option is selected, only users with unique ID numbers will be imported. If a user ID within the export file conflicts with a user currently enrolled within the database, the user will not be imported and the import rejection logged.

#### 22.3.3.1.2 Reject duplicate CardID numbers with unmatched names.

If this option is selected, imported users with conflicting ID numbers will be discarded if their name cannot be matched to the user currently enrolled within the database. If an existing user has both the same ID number and name, the imported image set will be merged with the image set currently stored within the database.

### 22.3.3.2 Import Log

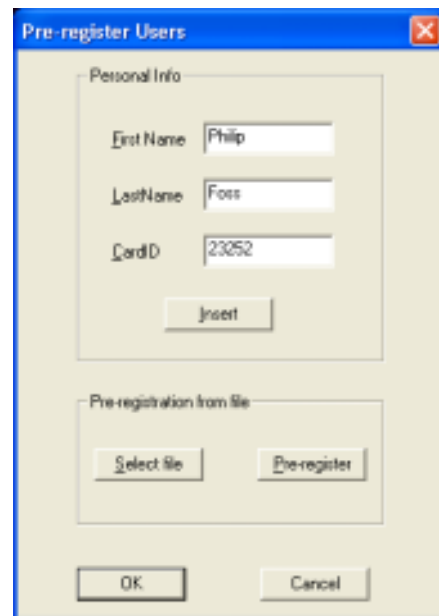
The progress of the import is saved to a text file. Any rejections will appear in the import log. The import log resides on the server and stored as "importuserslog.log".

## 22.3.4 Regenerating Templates

Select **Retrain All** from the *File* menu of the Edit Database window in order to clear all biometric templates and regenerate (i.e. train) the templates across all users currently stored within the Discovery database. Once a retraining operation has begun, the biometric templates across all users are cleared, and a classification or verification operation will not function until all templates have been regenerated. Regeneration of templates requires approximately 10 seconds per user.

## 22.3.5 Pre-Registration of Users

Users may be added (registered) within the Discovery database without performing an enrollment operation (i.e. facial image collection). This operation is referred to as pre-registration. Pre-registered users are enrolled at a later time, through use of either the Wiegand interface (i.e. card reader or keypad device) or the "Add" push-button control located on the main screen.



To pre-register a user or group of users select **Pre-register User** from the Database menu. The following Pre-Register Users window will appear.

**Figure 25. Pre-register Users dialog.**

**For pre-registering a single User:**

- Enter the User's first name in the **First Name** box.
- Enter the Users last name in the **Last Name** box.
- Enter the last 5 digits of the User's card number in the **Card ID** box.
- Click **Insert**.

The single User will be added to the database, however a biotemplate or enrollment images will not exist for that User.

To pre-register a group of Users:

- Click the **Select File** button. An "Open File" dialog control will be shown.
- Select the name of the file containing the User information and click **Open**.
- Click the **Pre-Register** button to import the list of User names and ID numbers.

The file containing the Users must contain 7-bit ASCII text only. Each line must be terminated by a carriage-return line-feed pair. Each line in the text file represents one User. Each line contains last name, first name, and card number delimited by commas as follows:

**Sample User file.**

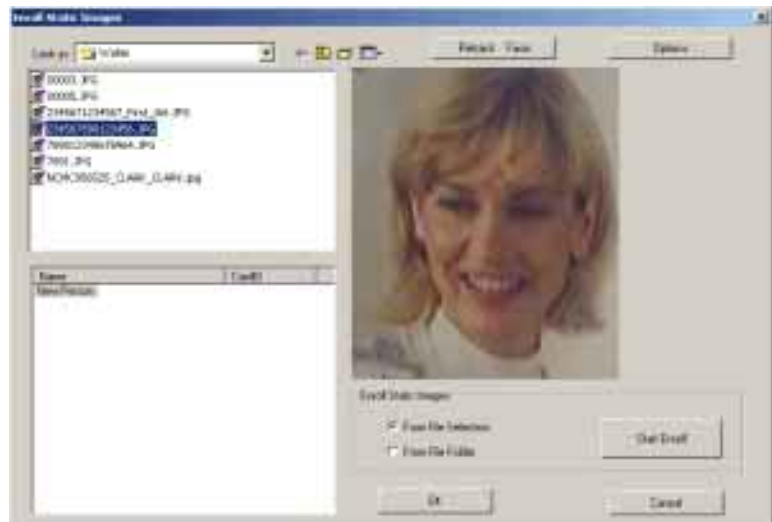
```
Chen, Jack, 38169
Foss, Philip, 38163
Sandler, Gregory, 22283
```

## 22.4 Enrolling from Static Images

The Discovery system includes facilities to import static JPEG images from a file, and apply these images for enrollment (template generation). Ideally, multiple images should be enrolled in order for the system to perform verification or classification operations reliably. Enrollment of static images may be performed in conjunction with the standard video enrollment procedure.

To perform an enrollment from static images, select **Enroll Static Images** from the *Database* menu.

**Figure 26. Enroll Static Images window.**



### 22.4.1.1 Enrolling a New User from a Static Image

A new user may be enrolled from a static image. The system will automatically assign the new users name and card number based on the filename of the JPEG. The JPEG file name must have the following format:

```
[ LASTNAME ] _ [ FIRSTNAME ] _ [ CARDID ] . jpg
```

For instance, a JPEG file with the name "Doe\_John\_25463" will create a user named John Doe, with ID number 25463.

To enroll a new user from a static image:

- Select **From File Selection**.
- Select the JPEG file from the file list located in the upper left corner of the dialog.
- Select **New User** within the user list.
- The JPEG image will appear in the image box. The person's face will be tracked automatically. If no tracking box appears around the face, click the **Retrack Face** button
- When the face is located in the image, click the **Start Enroll** button.

#### **22.4.1.2 Adding a Static Image to an Existing User**

You may add static images to the training set of an existing user. Files used to add images to existing users do not require the file name format indicated above.

To enroll a static image for an existing user:

- Select **From File Selection**.
- Select the JPEG file from the file list in the upper left corner of the dialog.
- Select the target users name in the user list box.
- The JPEG image will appear in the display screen located on the right side of the dialog. The users face will be tracked automatically. If no tracking box appears around the face, click the **Retrack Face** button
- When the face is located in the image, click the **Start Enroll** button.

#### **22.4.1.3 Batch Enrolling of Static Images**

Multiple users may be enrolled in batch mode from a set of JPEG images. Each image that is enrolled will create a new user within the system. The system will automatically assign each new users name and card number based on the filename of each JPEG file. The JPEG file names must have the following format:

[LASTNAME]\_[FIRSTNAME]\_[CARDID].jpg

For instance, a JPEG file with the name "Doe\_John\_25463" will create a user named John Doe, with card number 25463.

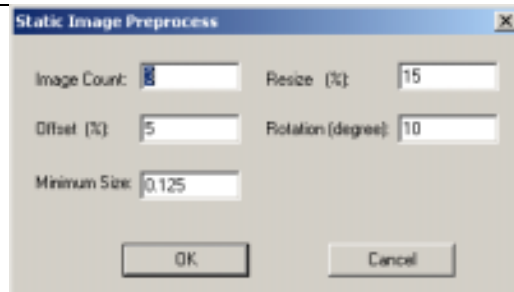
To enroll multiple users from static images in batch mode:

- Select **From File Folder**.
- Select the folder containing the JPEG files from the file list in the upper left corner of the dialog.
- Click the **Start Enroll** button to initiate enrollment of all users stored within the file folder.
- 
- The system will report if it was unable to locate a face in any of the JPEG images. If the system is not able to locate a face or the assigned ID number is currently used, it will not perform the enrollment operation for that image file. Following batch enrollment, the system will report the number of users enrolled and list the images that could not be enrolled within the file `EnrollStaticImage.log`.

#### 22.4.1.4 Options

Image preprocess options for the enrollment of static images may be modified by clicking on the "Options" button located above the main display panel. This will activate the following form:

Figure 27. Static Image Preprocess dialog.



The form shown above displays the recommended settings and each setting is described as follows:

##### 22.4.1.4.1 Image Count

Multiple images are generated from the segmented face. These generated images are randomly rotated, resized and offset in terms of vertical and horizontal placement using the settings provided on this form.

##### 22.4.1.4.2 Offset(%)

Establishes the degree of vertical and horizontal offset, expressed as a percentage of the segmented facial region.

##### 22.4.1.4.3 Resize(%)

Establishes the resizing range, expressed as a percentage of the segmented facial region.

##### 22.4.1.4.4 Rotate(degree)

The facial image is randomly rotated within the specified bounds.

##### 22.4.1.4.5 Minimum Size

The minimum size that is used for scanning facial images (specified as a ratio of full screen height).

### 22.5 Activity Log Viewer

The Activity Log Viewer displays all events that have occurred within the Discovery Client/Server installation. Included in the log report is the time and date in which the event occurred, the Discovery client machine at which the event occurred, the associated user name (if any) and type of event. The Log also records an image from the client when the event occurs.

The activity events that are recorded within the Log are as follows:

- Enroll Failure (Face)
- Enroll Success
- Reenroll
- Verify Failure (Face)
- Verify Success
- Face Classified
- Face Unknown

Multiple activity logs data may be viewed using the multiple document interface. Each view may be filtered to list events by event date, client computer, User name, and event type.

The Activity Log may also be saved or restored from a delimited text file.

### 22.5.1 Showing the Activity Log

In order to display the activity log, perform the following operations:

- Click the Windows **Start** button.
- Select **Discovery Log Viewer** from the *Start* menu.
- Click **OK** on the "Display Filter" window. The Discovery Log Viewer will open showing all activity events.

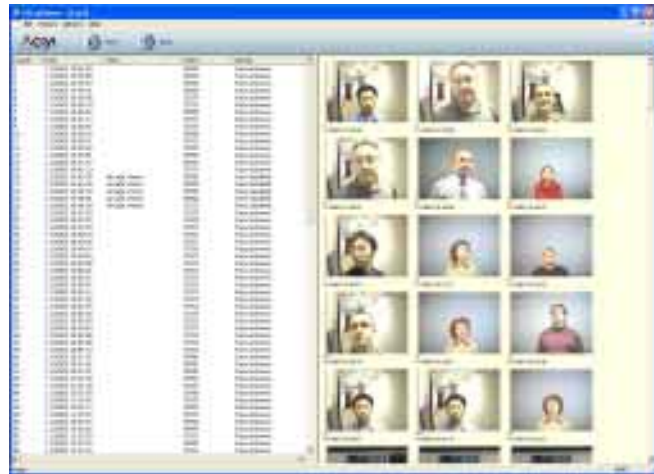


Figure 28. Discovery Log Viewer window.

### 22.5.2 Filtering an Existing View

To filter the events in an existing view, select the view that you want to filter, then select **Filter** from the *Window* menu, or click the **Filter** button. The following Activity Log Filter dialog will appear.

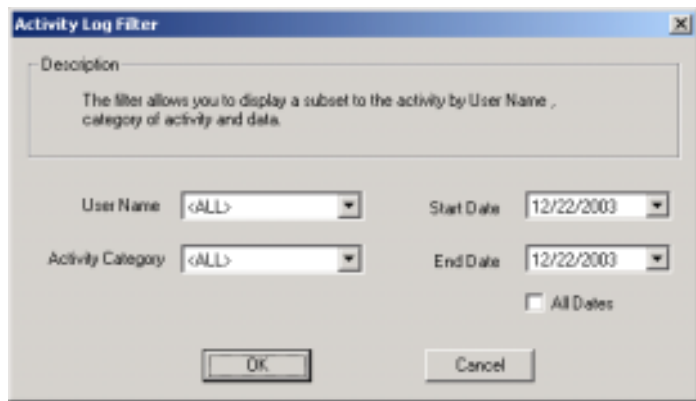


Figure 29. Activity Log Filter dialog.

- Select the filter criteria. You may filter on a single User name, Client Computer, the Activity Category or range of dates. Selecting multiple criteria will form a union of all selected filter criteria.
- Click **OK**. The view will filter the events based on the selected criteria.

### 22.5.3 Opening a New View

To open a new window with a different filter, select **New** from the *File* menu in the Log Viewer, or click the **New** button. The Activity Log Filter dialog will appear. Select the filter criteria then click **OK**. The new view will open in a new window.

### 22.5.4 Saving the Activity Log

The data from the current view can be exported to a text file for later viewing. Note that images are not exported when saving the activity log. To export the activity log perform the following operations:

- Select the view that contains the data to be exported.
- Select **Save** from the *File* menu. A standard File dialog will appear.
- Enter the name of the file used to save the activity log. If you choose an existing file, it will be overwritten.
- Click **OK**. The activity log will be saved to the specified file. Activity log files have the ".log" extension.

### 22.5.5 Loading the Activity Log

The data from an activity log file can be loaded into an existing view. To load an activity log perform the following operations:

- Select the view that will receive the activity log data. Note that the loaded data will overwrite the current view's data.
- Select **Load** from the *File* menu. A standard File dialog will appear.
- Locate the activity log file to view. Activity log files have the ".log" extension.
- Click **OK**. The activity log file will be loaded into a new view.

### 22.6 Modifying Control Button Configuration

The buttons available on the control bar (Track, Classify, Verify, Add, 5 Closest, and Options) may be hidden to limit the functionality of the Discovery application.

To hide selected buttons on the control bar:

- Click the **View** menu.
- Select **Button Configuration** from the View menu.
- The *Button Configuration* dialog will appear.

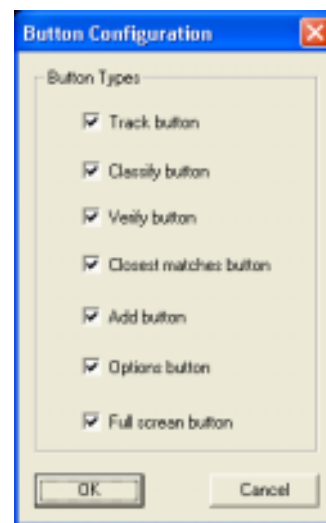


Figure 30. Button Configuration dialog.

- Select the buttons that will appear on the control bar.
- Click **OK**.

The Button Configuration dialog is password protected in the same manner as the Options dialog.

### 22.7 Setting Up Speech

By default, speech synthesis generated during enrollment and classification operations is disabled. Refer to section for details on how to activate speech.

Two modes of operation may be selected for speech generation, these being either a randomly selected speech string or a speech string that incorporates the User's first and last name.

To enter a new speech string or modify existing speech strings, open the SQL Server database called "FRSDiscovery" using a database editor such as SQL Server Enterprise Manager or DB Artisan. Open the database table entitled "HelloTable"



To create a new speech string type "RANDOM" into a blank record under the "Name" field. Following this, type in the speech string that you wish to add under the "Speech" field. Note that the phrase "Hello [First name], [Last Name]" will be added by default to all speech strings. Randomly selected speech strings are produced following classification of Users who have not been assigned user specific speech strings.

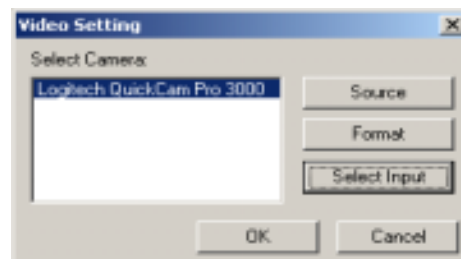
To assign a speech string directed toward a specific user, type first and last name into a blank record under the "Name" field. Following this type in the speech string that you wish to add for that specific user under the "Speech" field. Note that the phrase "Hello First/Last Name" will NOT be added to user specific speech strings.

If deleting a speech string, delete all text within the associated record of the database table entitled "HelloTable", and delete the "Wav2" entry for the same record.

### 22.8 Video Settings

Select **Video Settings** from the View menu to change video capture settings.

**Figure 31. The Video Settings window listing available devices.**



The video capture drivers provided by the I-CUBE FRS Discovery installation disk are shown in the above list box. The appropriate video capture driver is selected by highlighting the driver label and clicking OK.

Pushbuttons "Source" and "Format" bring up the driver settings forms that are specific to the selected driver. These forms vary dependent upon the video capture hardware that is installed. Refer to the video driver support documentation. "Select Input" is used by certain drivers for selecting either S-video or Composite input.

#### FRS Central Server

The FRS Central Server provides the basic face recognition functionality to the Discovery system. It must be running in order for the Discovery system to function.

### 22.9 FRS Server Manager

The FRS Central Server is installed and run on a single computer. While the FRS Central Server is running, the Server Manager icon appears in the application tray at the bottom of the screen.



To change the FRS Central Server settings, or shutdown the Server, double-click on the FRS Server Manager icon. The following FRS Server Manager window will appear.

The FRS Server Manager displays the name of the computer on which the FRS Central Server is running. The figure above shows the FRS Central Server is running on "DEMO". The status of the FRS Central Server is also shown. While the Server is running, the status will be "Started".

The FRS Server Manager also displays the number of Client Computers currently connected to the Server, the number of Training Servers used to generate the biometric templates (1 machine by default in the case of the Discovery System), and the FRS database currently in use.

From the FRS Server Manager window, you may shutdown and restart the FRS Central Server, view currently connected Client computers, add FRS Training Servers or select the FRS database to which you wish to establish a connection.

Clicking on the **X** button in the top right of the FRS Server Manager window will hide the window, but does not stop the FRS Central Server.

### 22.9.1 Shutting Down the FRS Central Server

To Shutdown the FRS Central Server, click on the **Shutdown** button. This will stop the Server's operations but not close the FRS Server Manager window. You can restart the FRS Central Server later. The status will read "Server Down".

### 22.9.2 Restarting the FRS Central Server

To restart the FRS Central Server after you have shut it down, click on the **Restart** button. The Central Server will initiate operations and the status display will change to "Started".

### 22.9.3 Viewing Connected Client Computers

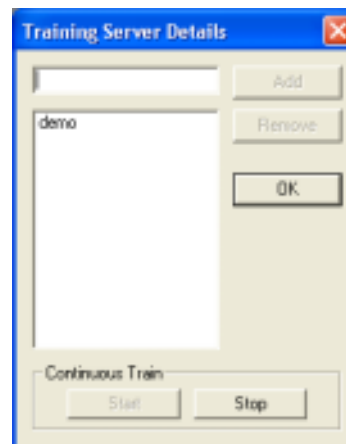
To see a list of all Client Computers currently connected to the FRS Central Server, click the ellipsis button (...) on the Client Computers line. The Client Details window will appear.

The Client Details window shows a list of all Client Computers currently connected to the FRS Central Server. Each item in the list shows the Client Computer name, and the time when it was connected.



### 22.9.4 Managing FRS Training Servers

Training servers are used in the generation of biometric templates from enrolled facial images. Click on the ellipsis button (...) on the FRS Training Servers line. The Training Server Details window will appear.



In the Training Server Details window, you can view the FRS Training Servers currently connected to the FRS Central Server, add and remove Training Servers, and control Continuous Training on each Training Server.

Having more than one Training Server connected to the FRS Central Server decreases the amount of time it takes to train (generate templates) for all individuals stored within the FRS database. The FRS Central Server automatically balances the training load between Training Servers.

#### 22.9.4.1 Adding a Training Server

To add a Training Server to the FRS Central Server, enter the name of the Training Server in the text box and click the **Add** button. The Training Server will be connected to the FRS Central Server and assigned training tasks.

### 22.9.4.2 Removing a Training Server

To remove a Training Server from the FRS Central Server, select the Training Server from the list of connected Training Servers, and click the **Remove** button. The Training Server will be removed and the training load will be shifted to the other Training Servers.

### 22.9.4.3 Controlling Continuous Training

The purpose of the Training Servers is to continuously update biometric templates using enrolled images. To stop continuous training on a Training Server, select the Training Server from the list of Training Servers, and click the **Stop** button. To start continuous training on a Training Server, select the Training Server from the list of Training Servers, and click the **Start** button.

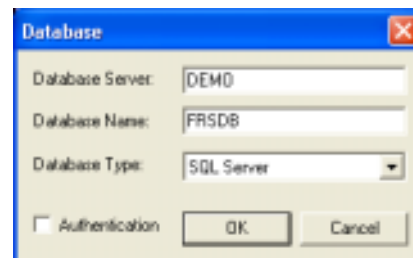
## 22.9.5 Selecting the FRS Database

The FRS Central Server may be connected to any FRS database on the network. The database provides biometric templates to the FRS Central Server (for use in the clients), and stores all enrolled facial images used in template generation.

The FRS Central Server can be connected to only one FRS database at a time.

To connect to a database, click the ellipsis button (...) on the Database line. The *Database* window will appear.

- Enter the name of the computer hosting the database in the **Database Server** box.
- Enter the name of the database itself in the **Database Name** box.
- Select the **Database Type** from the drop-down list.
- Click **OK**.



The *Database* window will close and the database name will appear in the *Database* box in the FRS Server Manager window.

Checking the **Authentication** box will force the user to enter a username and password each time that a connection to the database is attempted, i.e. each time FRS Central Server or FRS Training Server is started. Be aware that the username and password can be different for each database.

The default username is "frsuser" and the default password is "password."

Right-clicking on the FRS Server Manager tray icon will display a popup menu that allows you to show and hide the FRS Server Manager window, and shutdown and restart the Server. Selecting exit will not only hide the FRS Server Manager window, but stop the FRS Central Server itself.

## 22.10 FRS Training Server Manager

The FRS Training Server continuously updates biometric templates using the images that are enrolled for each user.



The Training Server(s) receive facial images from the FRS database, this transport layer is controlled through the FRS Central Server. After generating or updating a biometric template, the Training Server reads the template back into the FRS database via the FRS Central Server.

There may be multiple FRS Training Servers running simultaneously, each connected to the same FRS database through the FRS Central Server.

When a Training Server is running on a computer, the FRS Training Manager icon will appear in the tray.

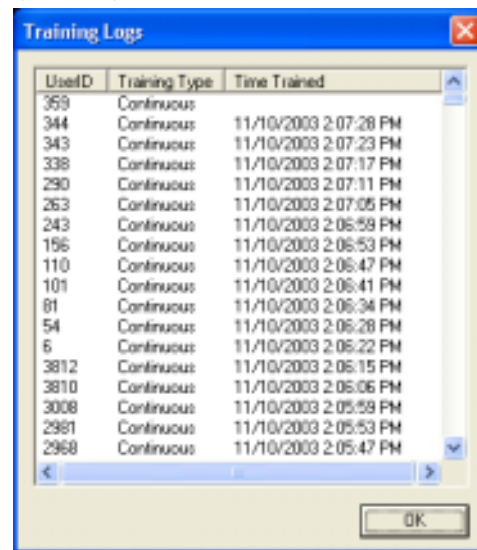
If the Training Server has been loaded, but not currently training the icon will be grayed.



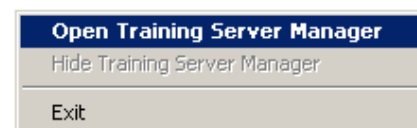
Double-click the following icon to display the FRS Training Manager window.

The FRS Training Manager window displays the name of the host computer that is running the Training Server, the ID of the individual whose template is currently being generated or updated, and the type of training that is being performed (background vs. continuous). Background training is performed once immediately following an enrollment or re-enrollment operation. Continuous training is performed continuously over all users currently enrolled within the system. To stop continuous training on the local Training Server, click the **OFF** button.

In the above example, the FRS Training Server is running on computer "DEMO", and user 81 is currently undergoing *continuous* training.



A log displaying the training history may be viewed by clicking the **Training Log** button. This log displays the user ID for individuals that have been most recently trained, the training method (i.e. background vs. continuous), and the time at which the biometric templates were trained (i.e. re-generated), as follows:



Control of the Training Server is also available by right-clicking on the FRS Training Manager tray icon. A popup menu will appear with the option to open and hide the Training Server Manager. Selecting **Exit** will close the window and stop the Training Server.

## 23 Biometric Intelligence 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.



### 23.1 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.

### 23.2 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:

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

### 23.3 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).

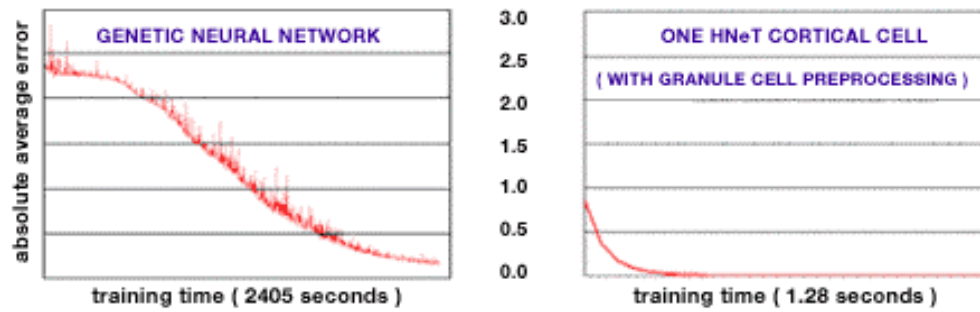
The holographic / quantum neural approach (HNeT) does not require a search process, and learns many orders of magnitude faster than traditional back-propagation or genetic based neural networks.



### 23.4 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.

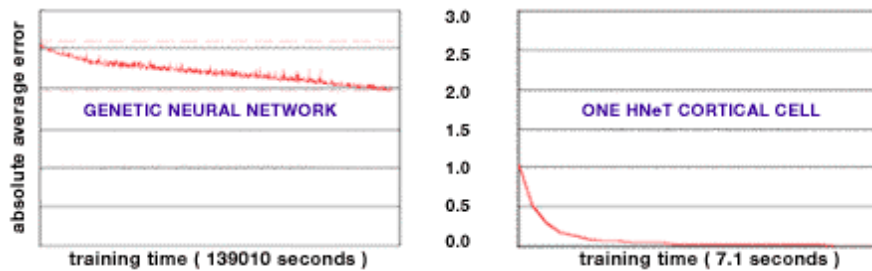


### 23.5 Comparison 1 – Learning 100 Stimulus-Response Patterns

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.

### 23.6 Comparison 2 – Learning 500 Stimulus-Response Patterns

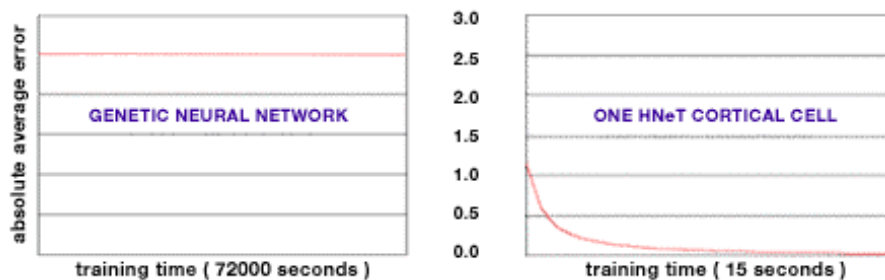
Increasing the number of stimulus-response patterns causes the genetic neural network to approach a state of saturation. At this level of



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.

#### 23.6.1.1 Comparison 3 – Learning 1000 Stimulus-Response Patterns

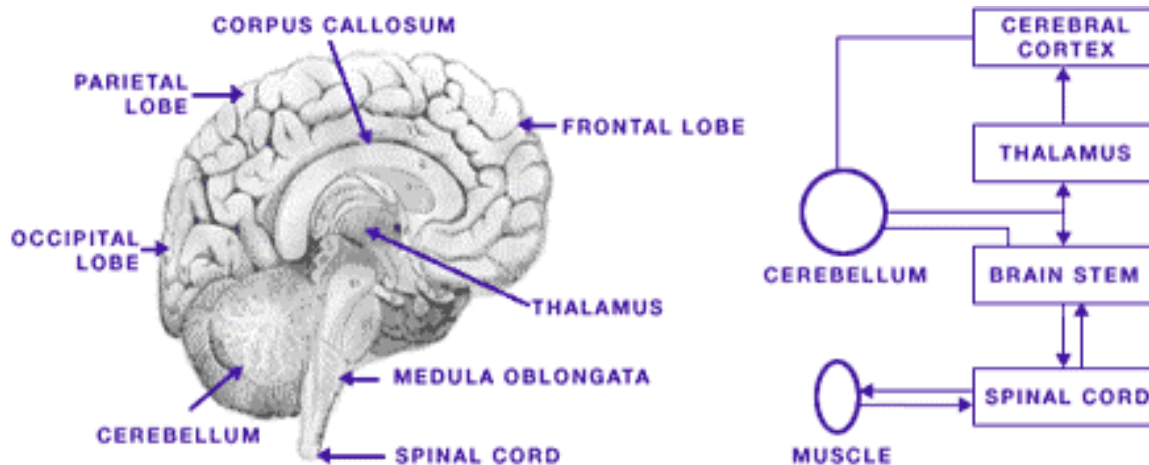
At 1000 stimulus-response patterns the genetic neural network is unable to achieve any measurable level of convergence, even after 20 hours of training. The rapid learning characteristic of the HNeT system is again unaffected by this increase in storage density.



### 23.7 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 (enfolding) 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 enfolding onto the same set of scalars (in other words - computer RAM).



## 24 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 enrollee, and he/she is incorrectly identified or verified by a biometric system as being that enrollee. 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 enrollee.

**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 it is unable to be read. A key is used to decrypt (decode) the encrypted biometric data.

**Enrollee** - 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 enrollee or fails to verify the legitimate claimed identity of an enrollee.

**False Rejection Rate/FRR** - The probability that a biometric system will fail to identify an enrollee, or verify the legitimate claimed identity of an enrollee. 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 enrollee identification attempts
NEVA	is the number of enrollee verification attempts

This estimate assumes that the enrollee 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 enrollee 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 enrollee.

**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 enrollee, 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 enrollee whose identity is being claimed, to determine whether it matches the enrollee's template. Contrast with 'Identification'.

**WSQ (Wavelet Transform/Scalar Quantisation)** - A compression algorithm used to reduce the size of reference

## 25 Special Terms and Conditions

This offer is subject to our standard conditions of agreement available on request

**Exchange Rate:** **Rate used:** **US\$ 1,00**

The prices quoted below are subject to exchange rate variations and will be based on 80% of the quoted price. Any variation from this rate of exchange on the date payment is received by us, within five (5) clear EDUCATIONAL FACILITYing days (the date selection will be at the discretion of I-CUBE, is for the account of the purchaser. The amount to be adjusted accordingly is 80% of the purchase price. The rates of exchange which will be applied will be those quoted by EDUCATIONAL FACILITYers nominated by I-CUBE

**Delivery Terms** : **Estimated 5 to 8 weeks from date of receipt of your payment.**

: See Below

**Validity** : This offer is valid for 30 days from the above date.

**VAT** : Prices "EXCLUDE" VAT

### General Terms and Conditions of Sale from I-CUBE

*The Purchaser of products from I-CUBE (Integrated Intelligent Imaging) (herein called "the Company") is bound by the general terms and conditions below. The General Terms and Conditions described herein, together with the Company's price list and/or proposal and/or any incorporated documents shall be read together as constituting the sales contract. IN THE EVENT OF ANY CONFLICT, THESE CONDITIONS OF SALE SHALL GOVERN.*

#### **1. LIMITED WARRANTY**

1.1 The Company warrants new goods sold hereunder to be free from defects in materials and workmanship, and to be of the kind and quality specified in the proposal, for a period of one year from the date of supply.

1.2 The Company makes no warranty whatsoever as to:

1.3 Any goods sold hereunder which have been repaired or altered by anyone other than the Company.

Goods manufactured by others, which may be incorporated with equipment installed or sold hereunder; however, the manufacturer's warranty for such goods shall be assigned to the purchaser, if possible.

1.4 Purchaser and the Company agree that purchaser's sole remedy against the Company and/or its suppliers for any defects in the goods sold hereunder, whether purchaser's claim arises under the warranty set forth above, or otherwise, shall be limited to the repair or replacement, at the Company's option (during normal working hours) of any parts, FOB the Company's source of the parts. The Company shall have no obligation to pay for installation, or removal of said parts.

1.5 If goods manufactured or sold by the Company are installed, or installation is supervised by the Company or an authorized agent, the warranty period shall commence upon completion of installation, provided installation is not unreasonably delayed by purchaser, in which event the warranty period shall commence when installation could have been completed absent such delays. On all other goods, the warranty period shall commence upon tender of delivery to Purchaser.

## 2. SOFTWARE LICENSE

- 2.1 GRANT OF SOFTWARE LICENSE. The Company grants a limited, non-exclusive license to use (not own) one copy of the purchased software per unique computer under the Licensee's custody or control, and subject to the following restrictions and conditions of this Agreement.
- 2.2 Sole Remedy. The sole remedy of the Licensee for any damages related to use of the software shall be the replacement of the software or a refund of the value of the software, at the Company's option, provided that the Licensee notifies the Company in writing within one year of the purchase date.
- 2.3 Updates. The Company will provide Software maintenance and/or updates for a period of one year from the purchase date. Thereafter, should the Company elect to provide maintenance or updates, the Company may charge a fee (in an amount determined by the Company) for such products or services, or may waive said fee at its sole election.
- 2.4 TITLE TO SOFTWARE. All title, copyrights and trademarks in and to the Software including any accompanying printed material, and any copies of the Software, and all enhancements, modifications and updates to the Software, are owned by the Company.

## 3. DELIVERY and SCHEDULE

- 3.1 Dates of shipping, delivery, or completion, as may be stated in the Company's proposals, are approximate and assume prompt receipt of all necessary information and reasonable cooperation from purchaser. Delivery schedules are set from the date of receipt of system down payments.
- 3.2 The company shall not be liable for delay in its performance of the contract, due to force majeure or causes beyond its reasonable control. In the event of any such delay, date of delivery shall be extended for a period of time equal to that lost by reason of the delay.

## 4. COMPANY DESIGNS and STANDARDS

- 4.1 Because the Company is constantly improving its products, the designs, dimensions, and weights shown in its proposals, while sufficiently accurate for most purposes are subject to variation. If extreme accuracy is required, additional information and certification will be provided upon request after receipt of order.
- 4.2 The goods sold hereunder shall be manufactured to the applicable standards, if any, stated in the proposal documents. In the absence of definite descriptive design criteria, the Company's standards shall be applicable.

**Basic Terms & Conditions**

- VALIDITY : 90 DAYS [Valid until 2005-08-19]
- AGREEMENT : This quotation is subject to the "Standard Conditions of Agreement" attached to the quotation. If, for any reason, this agreement is not attached to the quotation, a copy will be supplied on request.
- SHIPPING METHOD : Courier
- DELIVERY BASIS : Delivered
- DELIVERY TIME : Approximately 5 to 8 weeks. Not firm.
- QUOTATION BASIS : Exclusive of VAT, import duties, surcharges, excise duties and any other ad valorem costs as specified in the Customs and Excise Act No 91 of 1964 and Amendments thereto, are excluded.
- "Ordinary Customs Duty" means any duty specified under Part 1 of Schedule 1. "Import Surcharge" means any duty leviable under Part 4 of Schedule 1. "Ad Valorem Customs Duty" means any duty specified under Part 2, Section B of Schedule 1. However, if these ad valorem costs are quoted, they should be considered only as a guideline of the costs ruling on the date of quotation. If applicable, these amounts will be invoiced and documentary evidence provided.
- RATE OF EXCHANGE : US\$1,00  
Any variation from this rate of exchange on the date payment is received by us, within five (5) clear EDUCATIONAL FACILITYing days, the date selection will be at the discretion of Protea Electronics (Pty) Limited, is for the account of the purchaser. The amount to be adjusted accordingly is 80% of the purchase price. The rates of exchange which will be applied will be those quoted by the EDUCATIONAL FACILITYers nominated by I-CUBE.
- EXPORT LICENCES : Delivery and export from country/countries of origin of items requiring export licenses is subject to these being granted by the governments of the country/countries of origin.
- WARRANTY : See "Limited Warranty" from I-CUBE above  
The seller warrants products against defective material and/or poor workmanship.
- PAYMENT TERMS : Prepayment - See payment terms from I-CUBE above
- E. & O. E.

## 26 INDEMNITY

*The person or Company listed above agrees to indemnify, hold harmless and defend I-CUBE and its officers, employees, agents and representatives from and against:*

*Any liability, loss and expense arising by reason of claims by government, provisional, municipal, local or other authorities (including Suppliers of equipment) or any failure of those listed to comply with any Act of Parliament, law, ordinance, regulation or bye-law made with lawful authority by a government, provincial, municipal, local or other authority, provided that compliance by those listed with the above is required under the provisions of this Document, at law, or otherwise, including without limitation, failure of those listed to pay taxes, duties or fees; and*

*Any claim, liability, loss or expense arising from actual or asserted infringement or improper appropriation or use by those listed of trade secrets, proprietary information, know-how, copyright rights (both statutory and non-statutory) or patented or unpatented inventions or actual or alleged unauthorised imitation of the WORK of others arising out of the use or sale of materials, equipment, methods, processes, designs, information, or other things including construction facilities furnished those listed or its nominated personal in or for performance of the WORK; and*

*Any claim, demand, cause of action, loss, expense, or liability on account of injury to or death of persons (including the employees of the I-CUBE) or damage to or loss of property including the property of the OWNER arising directly or indirectly out of the acts or omissions to those listed or its SUB Contractor's or the employees or any thereof, in the performance of the work, including without limitation, such claims, loss of liability arising from the use or operation by those listed of construction equipment, tools, scaffolding, or facilities furnished to those listed by I-CUBE to perform the work, irrespective of whether party to be indemnified was concurrently negligent, whether actively or passively, and including any expenses and attorney's fees incurred by I-CUBE for legal action to enforce those listed indemnification obligations under this clause, but excepting where the injury or death of persons or damage to or loss of property was caused by the sole negligence or wilful misconduct of the party to be indemnified; and*

*Any claim, demand, cause of action, loss, expense or liability on account of actual or alleged contamination, pollution, or public or private nuisance, arising directly or indirectly out of the acts or omissions to act of those listed or its SUBCONTRACTORS in the performance of the WORK.*

Proposal for  
PORT

for

# ADVANCED VEHICLE ACCESS CONTROL SOLUTIONS

## Incorporating LICENSE PLATE RECOGNITION, DIGITAL RECORDING and Biometric Facial Identification / VERIFICATION SOLUTIONS

*Compiled / Supplied by*

Dawa Sewbalak

**Power Automation**

E-Mail: [power.auto@intnet.mu](mailto:power.auto@intnet.mu)



Sunday, 29 May 2005

*In conjunction with I-Cube*

