ADVANCED BIOMETRIC FACIAL IDENTIFICATION

USER MANUAL

BY

MARSHALL INTERNATIONAL

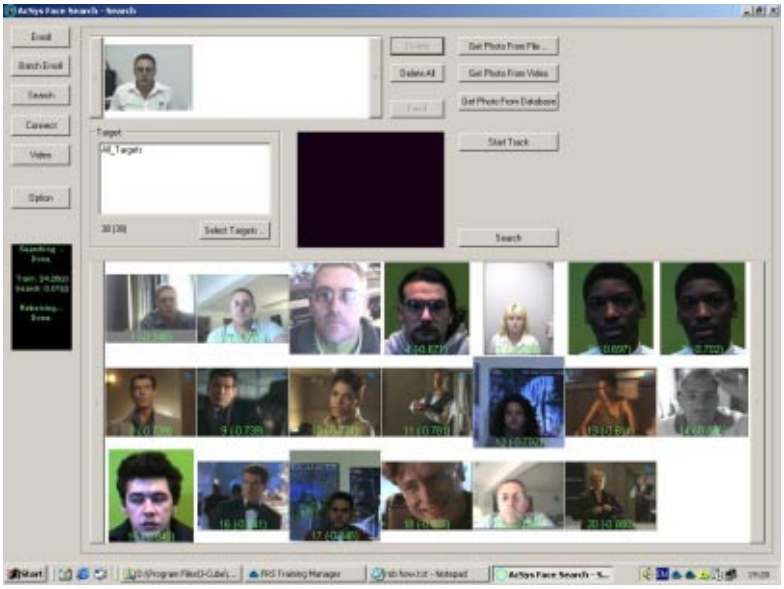
JANUARY 2005

Saturday, 15 January 2005

ADVANCED BIOMETRIC FACIAL IDENTIFICATION

This solution allows: -

- Image capture of the person from a high resolution colour camera;
- Face finding within the image;
- Linking of the face with various fields (such as ID no., name, Birth, Sex, Eye, hair Colour, Ht, Wt, Address, City, State, Zip, Country);
- Searching central database and display of results;
- Entry of all images and details that are not in the database;



This document describes the software and equipment, how to use it and how to connect it together that is required for a biometric facial identification system.

David Marshall
E-mail: david@marshall.co.za
MARSHALL INTERNATIONAL
89 Broadway Bez Valley Jhb.
P.O.Box 34501, Jeppestown, 2043
Tel:011 622-3660 Fax:011 622-2520
Website: www.marshall.co.za

Introduction

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

Recognition 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. Biometric recognition 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 security, marketing and technological viewpoint. MARSHALL INTERNATIONAL ADVANCED BIOMETRIC FACIAL IDENTIFICATION gives you the opportunity to have access to the full range of possibilities for biometric facial identification within your organization without a major up-front investment in software and hardware peripherals.

Features: Speed, accuracy and intelligence are among the key qualities that differentiate MARSHALL INTERNATIONAL products from other biometric technologies. SPEED: Using a revolutionary core technology called HNet, MARSHALL INTERNATIONAL Biometrics delivers cutting-edge security with basic hardware requirements and split-second processing times. ACCURACY: The MARSHALL INTERNATIONAL FRS (Face Recognition System) was the most accurate technology tested in the International Biometric Group's Comparative Testing for IT Security and E-Commerce (0% False Acceptance Rate (caught all impostors) at an excellent False Rejection Rate of just 3.1%). INTELLIGENCE: MARSHALL INTERNATIONAL **ADVANCED BIOMETRIC FACIAL IDENTIFICATION** learns, remembers and recognises. HNet emulates the human brain in structure and function, becoming more familiar with your face each time it

sees you, adjusting for difference due to aging and cosmetics without increasing the size of the biometric template.

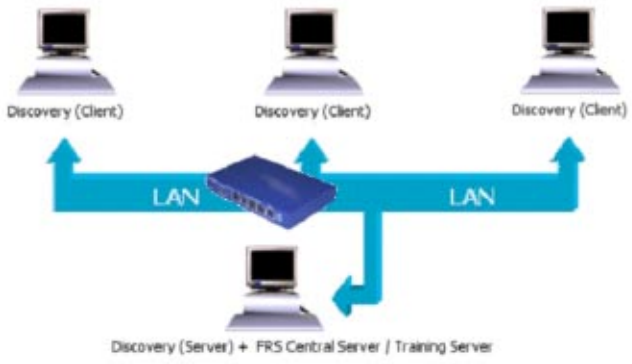
Benefits: The MARSHALL INTERNATIONAL product line offers powerful identity and verification technology for enterprises of all size and for third-party development.

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.

System Overview

The Acsys 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 Acsys Facial Identification Server and facial recognition operations may be performed on either Server or Client machines. The Acsys 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 the FRS Central Server and FRS Training Server, please contact Barry T. Dudley (082 562 8225, info@I-Cube.co.za).



System Requirements

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.

Acsys Facial Identification Client

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

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

Acsys 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

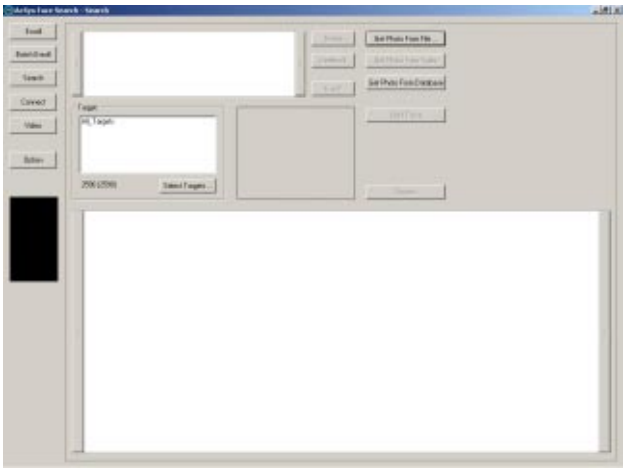
EQUIPMENT REQUIRED

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

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

FACIAL IDENTIFICATION SOFTWARE USER MANUAL

How to use AcSys Facial Search

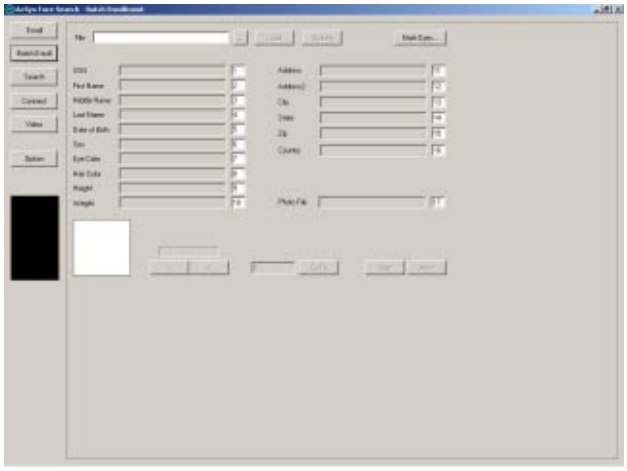


1. Enroll

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.

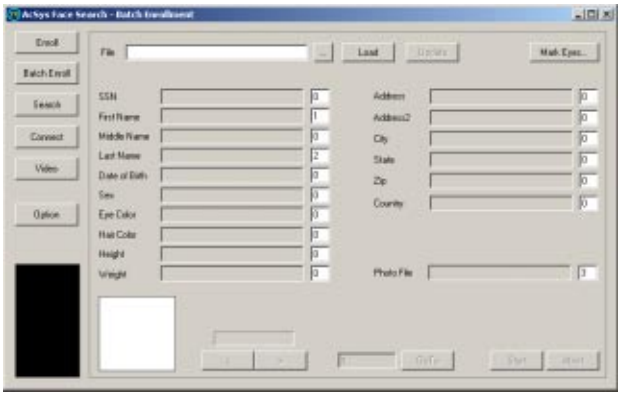
To enroll from vide, you have to enable video if there is no video displayed. You can do it by clicking “Video” button, which is located on left panel. Make sure you have camera and driver installed before doing that. You can adjust the video format and video source by clicking “Video” button again, 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.

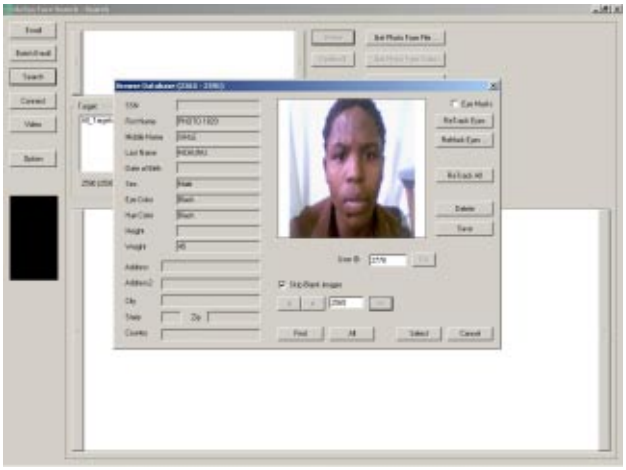
2. Batch Enroll



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.



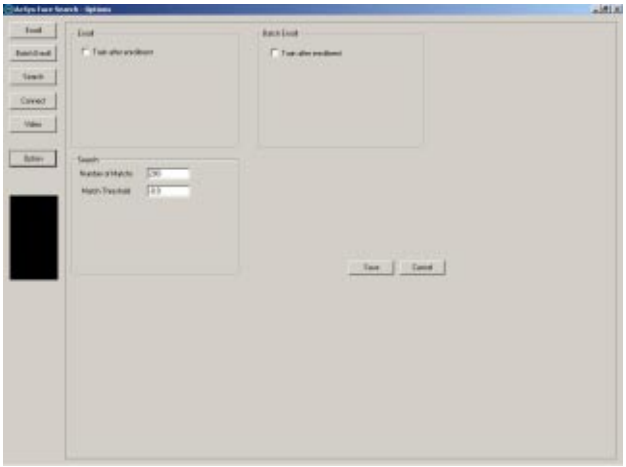
For example:
Bob, Smith, c:\images\jpeg\1.jpg
John, Brown, c:\images\jpeg\2.jpg

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 1st 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.

3. Search

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

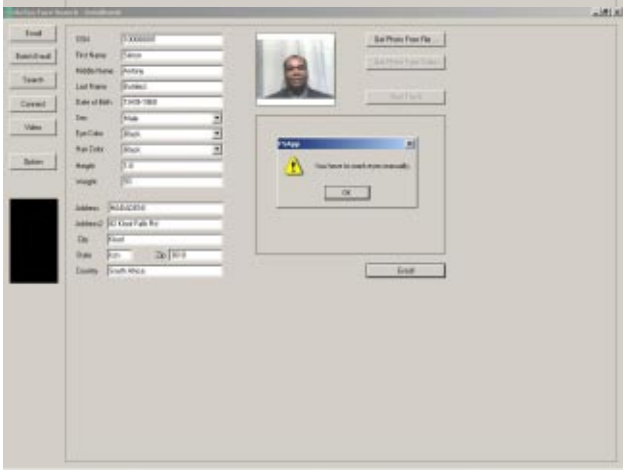
To search image from image file, click “Get Photo From File…” button, and select the image file.

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 that 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.

4. Browse Database

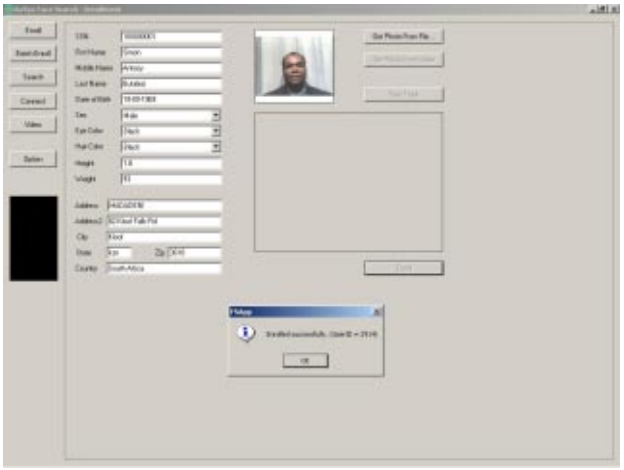
You can do quite a lot of things in browse database dialog box.

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.

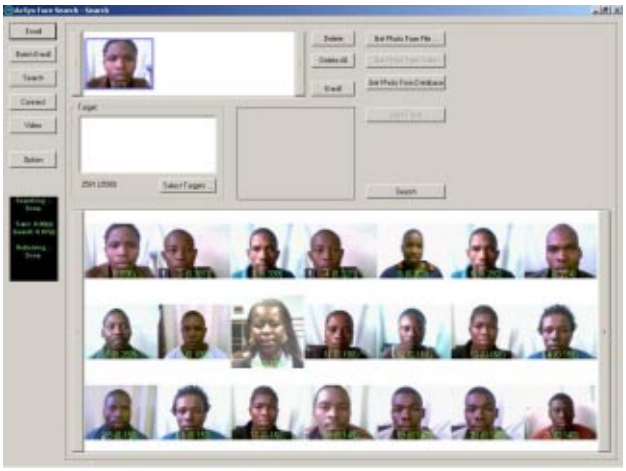
You can save this image to a jpeg file by clicking “Save” button, image will be save as [UserID].jpg.

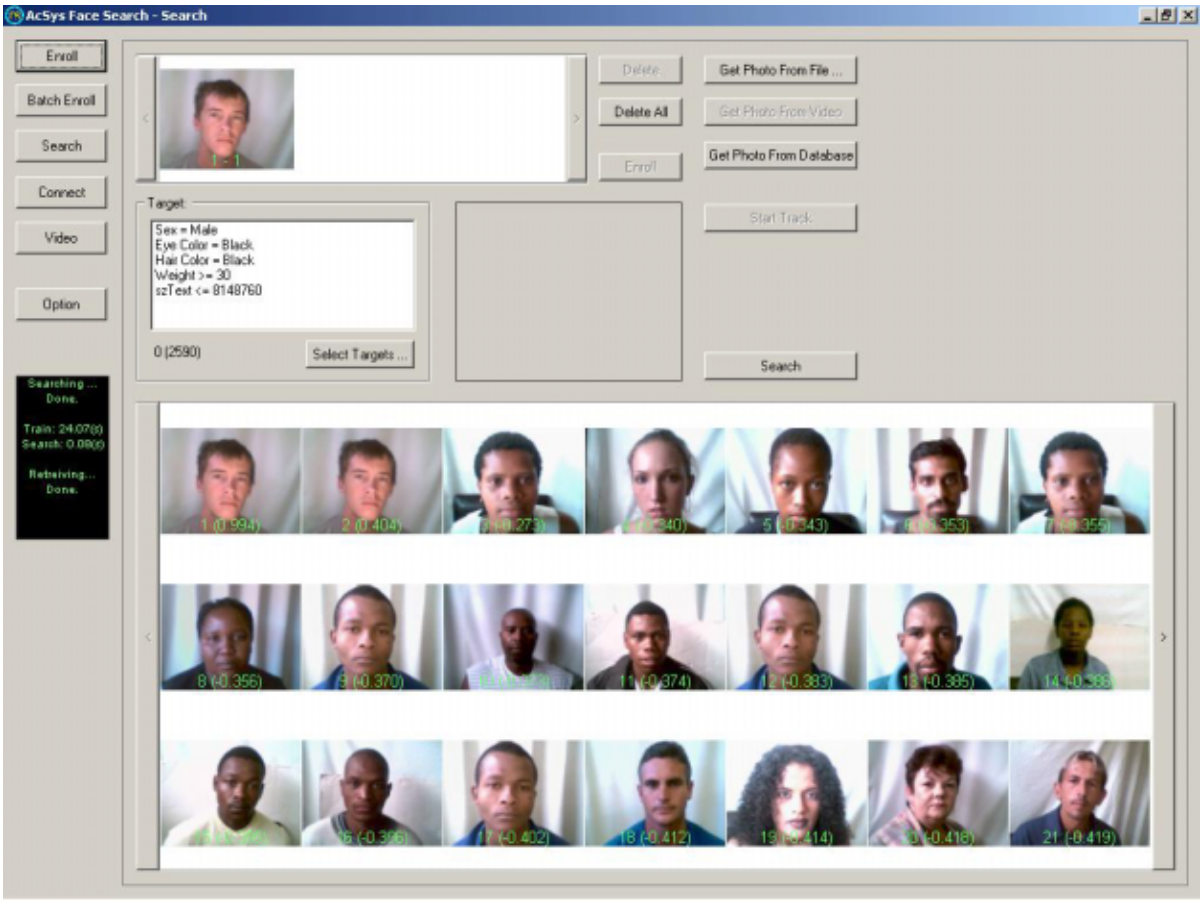
You can click “Find” button to find the images satisfied with certain condition. After that you can click “All” button to make it back to all dataset.

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.





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

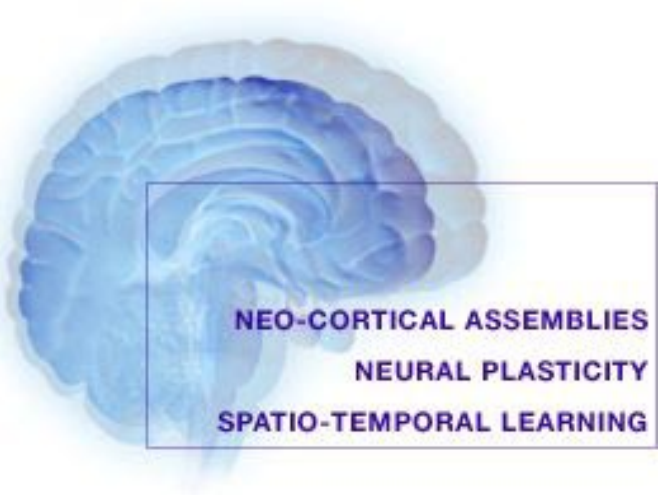
AND Corporation is the provider of **Application Development**

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

Overview

Biomimetic Intelligence is the science of understanding and replicating the processing mechanisms and structure of the brain. Traditional neural networks have little or no resemblance to actual neurological structures, and more importantly, have proven to be very limited in capability. The HNeT technology, however, applies the power of digital holography within synthetic neuron cells. Assemblies comprised of such cells have one-to-one correspondence with the primary cell structures of the brain. These biomimetic structures provide the capability for truly real-time learning, and present a vast increase in (stimulus-response) memory storage capacity.

To provide a practical example, a cell assembly can locate and track human faces in real time. A cell assembly can learn facial images in real time, building within its memory all observed forms of an individual, and subsequently identify that individual within a crowd, even determine facial expression such as smiling or frowning, etc. This application is at the upper limit of technological capability when employing traditional methods. Application of the basic two-cell "cerebellar" model reduces the above task to a rather straight-forward procedure. The HNeT technology is not limited to face tracking / identification, but may be similarly applied to numerous areas within the medical sector, process control, automation, defence, financial, etc.



HNeT Tools

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

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

Performance Features

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

A brief summary of the following performance features are covered:

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

General Comparisons

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

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

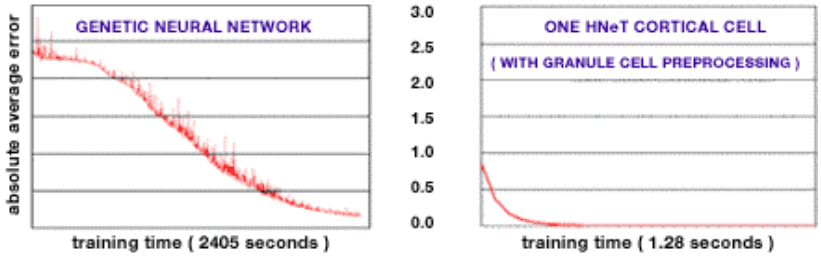
The Monte Carlo Test

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

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

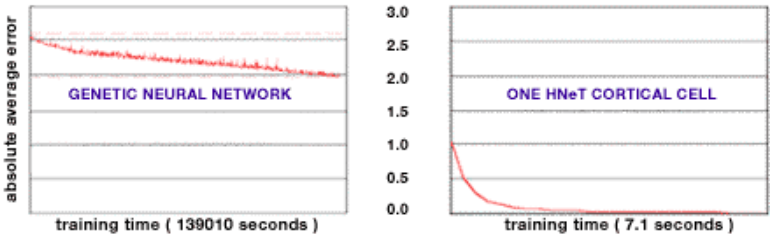
Comparison 1 – Learning 100 Stimulus-Response Patterns

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



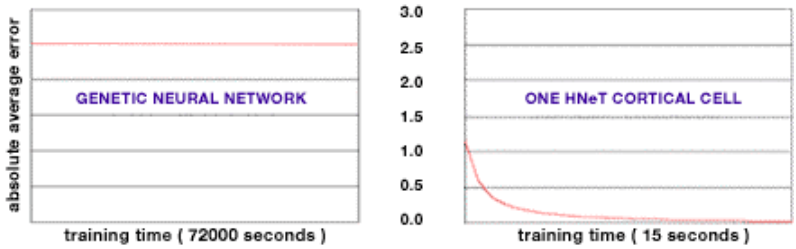
Comparison 2 – Learning 500 Stimulus-Response Patterns

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



Comparison 3 – Learning 1000 Stimulus-Response Patterns

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

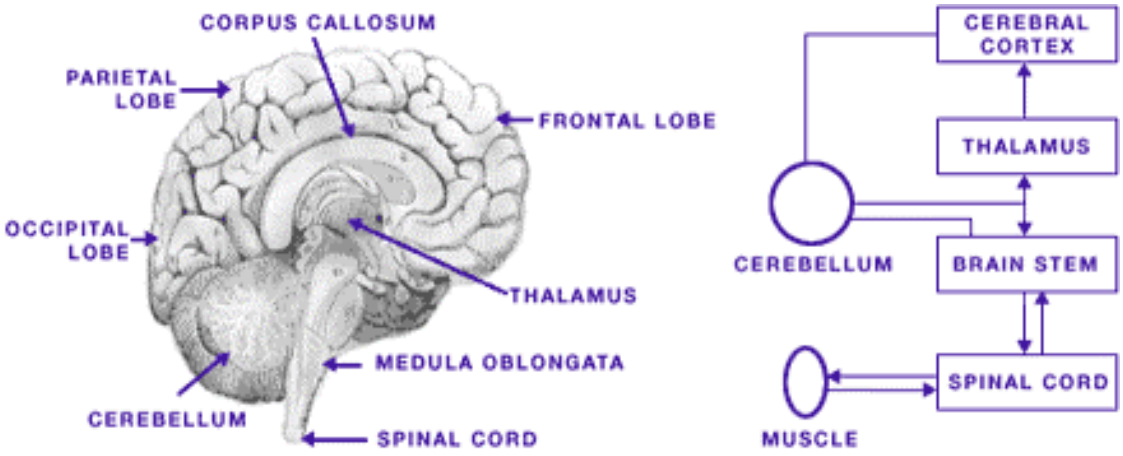


The Biology

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

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

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



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

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

Explanation of Biometrics

In order to work with the Acsys Facial Identification system, it is beneficial to understand the basic concepts of system operation.

Each User that is registered within the Acsys Facial Identification 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 identification of the user, applying the biometric template.

Tracking

In order to make face recognition non-intrusive and flexible, the Acsys Facial Identification 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 Acsys Facial Identification main window.

User Registration

Within the Acsys Facial Identification system, a user may be registered before they are enrolled. This means that users may be entered into the Acsys Facial Identification 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.

Definitions

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

Equal Error Rate - The error rate occurring when the decision threshold of a system is set so that the proportion of false rejections will be approximately equal to the proportion of false acceptances.
Extraction - The process of converting a captured biometric sample into biometric data so that it can be compared to a reference template.
Failure to Acquire - Failure of a biometric system to capture and extract biometric data (comparison data).
Failure to Acquire Rate - The frequency of a failure to acquire.
Failure to Enrol - Failure of the biometric system to form a proper enrolment template for an end-user. The failure may be due to failure to capture the biometric sample or failure to extract template data (of sufficient quality).
Failure to Enrol Rate - The proportion of the population of end-users failing to complete enrolment
False Acceptance - When a biometric system incorrectly identifies an individual or incorrectly verifies an impostor against a claimed identity.
False Acceptance Rate/FAR - The probability that a biometric system will incorrectly identify an individual or will fail to reject an impostor. The rate given normally assumes passive impostor attempts. The False Accept Rate may be estimated as FAR = NFA / NIIA or FAR = NFA / NIVA where

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

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

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

This estimate assumes that the enrolee identification/verification attempts are representative of those for the whole population of end-users. The False Rejection Rate normally excludes ‘Failure to Acquire’ errors
Field Test / Field Trial - A trial of a biometric application in ‘real-world’ as opposed to laboratory conditions.
Filtering - The process of classifying biometric data according to information that is unrelated to the biometric data itself. This may involve filtering by sex, age, hair colour or other distinguishing factors, and including this information in the database .
Goats - Biometric system end users whose pattern of activity when interfacing with the system varies beyond the specified range allowed by the system, and who consequently may be falsely rejected by the system.
Identification/Identify - The one-to-many process of comparing a submitted biometric sample against all of the biometric reference templates on file to determine whether it matches any of the templates and, if so, the identity of the enrolee whose template was matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity. Contrast with ‘Verification’.
Impostor - A person who submits a biometric sample in either an intentional or inadvertent attempt to pass him/herself off as another person who is an enrolee.

Live Capture - The process of capturing a biometric sample by an interaction between an end user and a biometric system.
Match/Matching - The process of comparing a biometric sample against a previously stored template and scoring the level of similarity. An accept or reject decision is then based upon whether this score exceeds the given threshold.
Multiple Biometric - A biometric system that includes more than one biometric system or biometric technology.
Neural Net/Neural Network - One particular type of algorithm. An artificial neural network uses artificial intelligence to learn by past experience and compute whether a biometric sample and template are a match.
Performance Criteria - Pre-determined criteria established to evaluate the performance of the biometric system under test.
Physical/Physiological Biometric - A biometric which is characterised by a physical characteristic rather than a behavioural trait. However, behavioural elements may influence the biometric sample captured.
Population - The set of end-users for the application.
Recognition - The preferred term is 'Identification'.
Record - The template and other information about the end-user (e.g. banned)
Response Time - The time period for a biometric system to return a decision on identification or verification of a biometric sample.
Score - The level of similarity from comparing a biometric sample against a previously stored template.
Template/Reference Template - Data, which represents the biometric measurement of an enrolee, used by a biometric system for comparison against subsequently submitted biometric samples.
Template Ageing - The degree to which biometric data evolves and changes over time, and the process by which templates account for this change.
Template Size - The amount of computer memory taken up by the biometric data.
Third Party Test - An objective test, independent of a biometric vendor, usually carried out entirely within a test laboratory in controlled environmental conditions.
Threshold/Decision Threshold - The acceptance or rejection of biometric data is dependent on the match score falling above or below the threshold. The threshold is adjustable so that the biometric system can be more or less strict, depending on the requirements of any given biometric application.
Throughput Rate - The number of end users that a biometric system can process within a stated time interval.
Type I Error - In statistics, the rejection of the null hypothesis (default assumption) when it is true. In a biometric system the usual default assumption is that the claimant is genuine, in which case this error corresponds to a 'False Rejection'.
Type II Error - In statistics, the acceptance of the null hypothesis (default assumption) when it is false. In a biometric system the usual default assumption is that the claimant is genuine, so this error corresponds to a 'False Acceptance'.
User - The client to any biometric vendor. The user must be differentiated from the end user and is responsible for managing and implementing the biometric application rather than actually interacting with the biometric system.
Validation -The process of demonstrating that the system under consideration meets in all respects the specification of that system.
Verification/Verify - The process of comparing a submitted biometric sample against the biometric reference template of a single enrolee whose identity is being claimed, to determine whether it matches the enrolee's template. Contrast with 'Identification'.
WSQ (Wavelet Transform/Scalar Quantisation) - A compression algorithm used to reduce the size of reference templates.