

# INTRODUCTION TO FACIAL RECOGNITION

*Compiled by Barry T. Fryer Dudley*

APRIL 2007

Supplied by



# TABLE OF CONTENTS

- 1 Introduction..... 3
  - 1.1 FACE RECOGNITION SYSTEMS ..... 4
- Explanation of Biometrics ..... 5
- 2 Biometric Intelligence Overview ..... 6
  - 2.1 HNeT Tools..... 6
  - 2.2 Performance Features ..... 7
  - 2.3 General Comparisons ..... 7
  - 2.4 The Monte Carlo Test ..... 7
  - 2.5 Comparison 1 – Learning 100 Stimulus-Response Patterns ..... 8
  - 2.6 Comparison 2 – Learning 500 Stimulus-Response Patterns ..... 8
  - 2.7 The Biology..... 9
- 3 Overview of Facial Software .....10
  - 3.1 System advantages .....10
- 4 Privacy discussion .....13
- 5 Equipment Requirement .....14
- 6 NEXT STEP .....14
- 6 Definitions.....15



**Copyright and Confidentiality Notice**

*Material contained in this document is proprietary to I-Cube (Integrated Intelligent Imaging) and is to be treated confidentially by all recipients. Acceptance of delivery of this material constitutes acknowledgment of the confidential relationship under which disclosure and delivery are made. No part of this publication may be reproduced or transmitted in any form or by any means, electronic or mechanical, including photocopy, recording, or any information storage and retrieval system without permission in writing from I-CUBE, MADADENI 82 Kloof Falls Rd, Kloof 3610, KZN, South Africa.*

## 1 Introduction

There is an ever-increasing requirement to remove the opportunity for fraud and crime and to ensure deterrents are in place to increase safety and minimize risk. The predictive ability enabled by the introduction of facial recognition enables potential thefts to be anticipated

The Facial solution proposed captures images of the person from the CCTV system and uses these images against the enrolled database. An accurate audit trail of each of these transactions is maintained for review. This solution ensures that only allowed workers are permitted to enter, their historic details are known as there is a system verification that is captured and a log of the images is maintained. This approach makes it possible to have an accurate and auditable record of every person that has entered or left the premises.



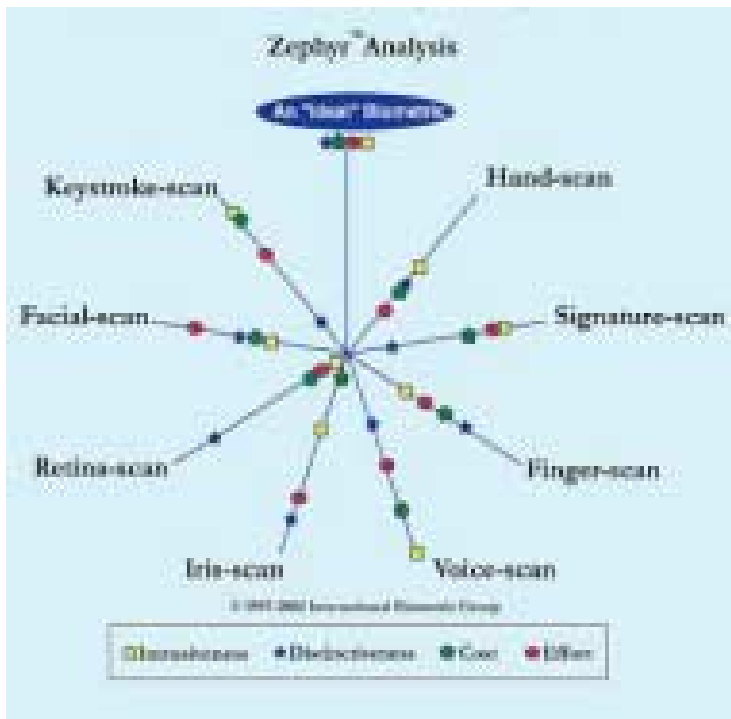
## 1.1 FACE RECOGNITION SYSTEMS

"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.



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

## Explanation of Biometrics

In order to work with the I-cube Facial VERIFICATION system, it is beneficial to understand the basic concepts of system operation.

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

Biometric VERIFICATION 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.

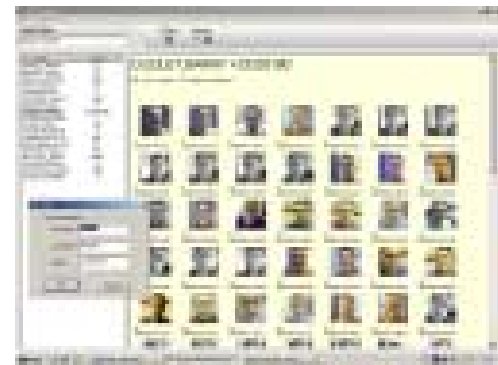
### Tracking

In order to make face VERIFICATION non-intrusive and flexible, the I-CUBE 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 continues automatically and continually, utilizing the HNET engine.



### User Registration

Within the I-CUBE Facial VERIFICATION system, a user may be registered before they are enrolled. This means that users may be entered into the I-CUBE 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.

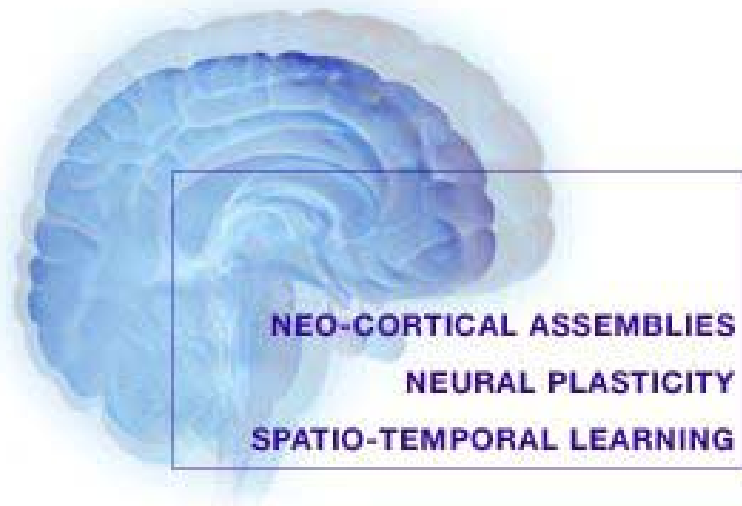
### Template Generation

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.

## 2 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.



### 2.1 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.

## 2.2 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:

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

## 2.3 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.

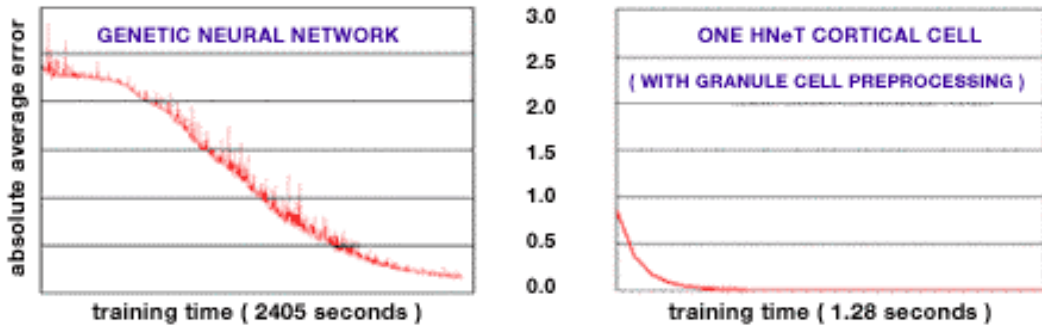


## 2.4 The Monte Carlo Test

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.

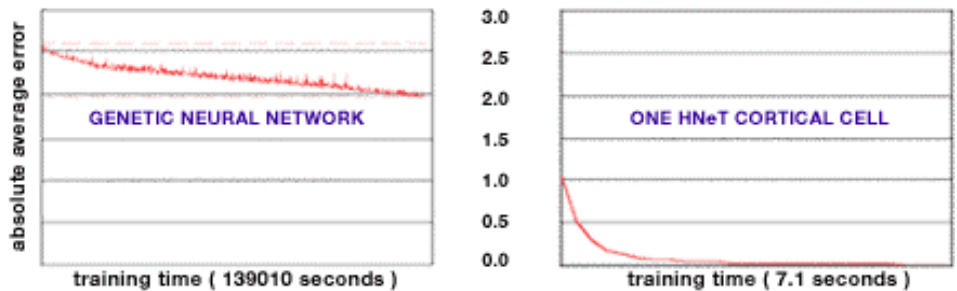


### 2.5 Comparison 1 – Learning 100 Stimulus-Response Patterns

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.

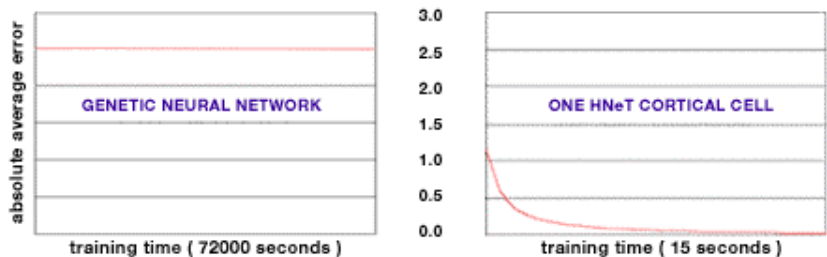
### 2.6 Comparison 2 – Learning 500 Stimulus-Response Patterns

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.



#### 2.6.1.1 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.



## 2.7 The Biology

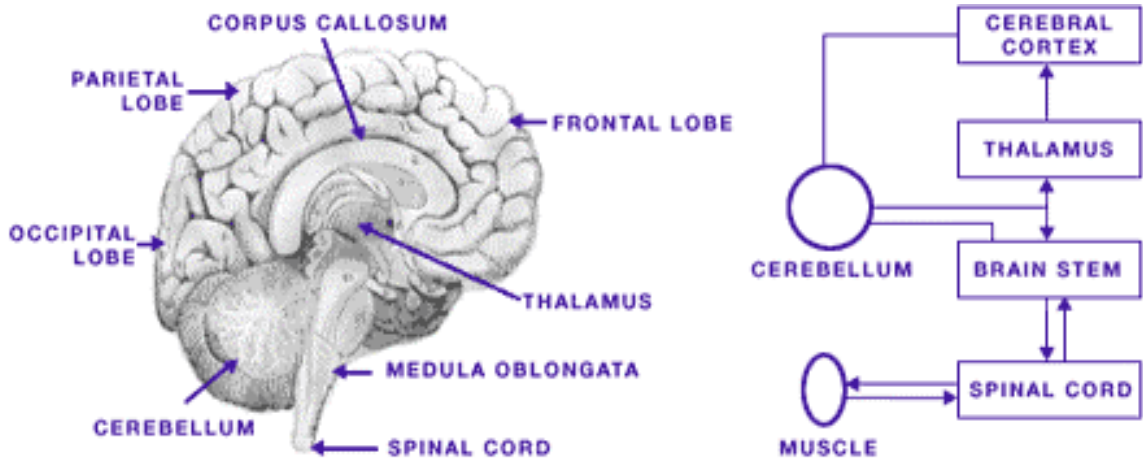
The following provides an overview of HNeT biomimetic intelligence. Biomimetic intelligence models cell inter-connectivity and signal processing aspects of actual neuron cell assemblies within sections of the brain referred to as the neo-cortex (gray matter or outer layer), the cerebellum (near the base 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 (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).Solution Proposed

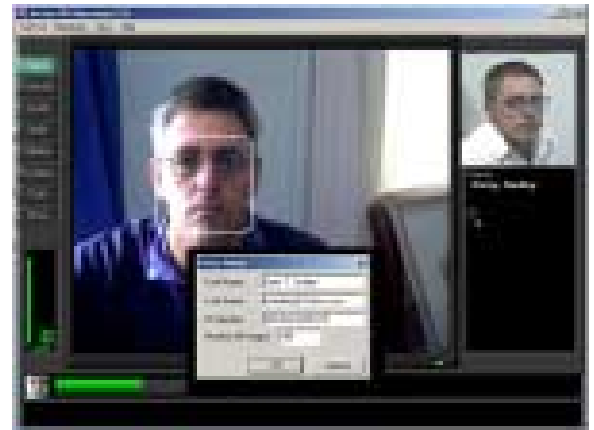


### 3 Overview of Facial Software

There is no doubt that BIOMETRICS, and particularly face recognition is fast becoming an important tool in the fight against crime. Statistics point to major reductions in the amount of crime where face recognition systems are installed. The proposed system provides facial verification that provides three-dimensional analysis of the person and then validates against the enrolled database.

The system provides the following leading-edge functionality:

- Tracking of multiple faces simultaneously in real time
- Enrolment of facial images from a live or recorded video stream
- Enrolment of facial images from a static image (JPEG)
- Identification (one-to-many authentication) from a video stream
- Verification (one-to-one authentication) from a video stream
- Database search for a specific individual



**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.

#### 3.1 System advantages

The system has the following advantages:

- Fully automatic process (no man-in-the-loop)
- Accurate capture
- Verifiable and auditable data
- Increases processing of the personal traffic at congested entrance
- The system collects the workers movement history



The system advantages over other automated solutions:

- Simple configuration (few cameras)
- Performs accurate facial verification and is not dependent on a face being presented exactly as it is in a photograph
- Simple integration into the existing computer resources (if required)
- Has a high recognition rate
- Has a user friendly display and operation
- A reliable system, low cost solution
- 24 hour operation not dependent on fatigue and inaccuracies
- Fast response (output in milliseconds)
- Facial recognition used for identification.





## 4 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.ibqweb.com/reports/public/reports/privacy\\_best\\_practices.html](http://www.ibqweb.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.

It is possible to have images in the database, which are not searched against, either for record purposes or just for logging purposes, for later review if a problem occurs.

## 5 Equipment Requirement

The software is compatible with Microsoft® Windows® VISTA. 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® VISTA

- 3 GHz Pentium 4, DUAL Processor
- 1 GB RAM
- 200 GB HDD
- WDM – compatible video capture device

### **I-CUBE FACIAL VERIFICATION Server**

- Microsoft® Windows® VISTA
- 3.4 GHz Pentium 4, DUAL Processor
- 2 GB RAM
- 1 TB HDD

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



## 6 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 templates.

