# The Open Biometrics Initiative and World Card

**Notes on RealTechSupport for Biometrics**

**Marc Böhlen, MediaRobotics Lab, University at Buffalo**

***Out-collect the data collectors***

**WhatTheHack2005, The Netherlands**

From the 4th IEEE Workshop on Automatic Identification Advanced Technologies, 10/2005 in Buffalo New York:

"We are evolving towards an age of convergence in identification technologies where everything that can compute has an IP address, every thing static has an RFID and every individual has a biometric identifier. AUTOID 2005 will bring together researchers, practitioners, and users from these converging fields to describe the state of the art and identify urgent open problems."

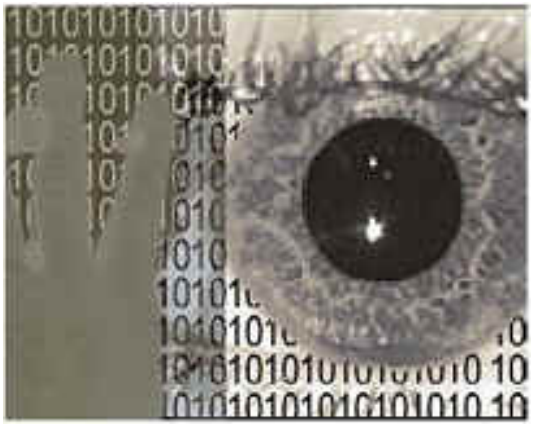


Fig. 1: Poster for the Biometrics Consortium Conference, 2004


Fig. 2: Time Magazine

# BACKGROUND INFORMATION

Typical Biometrics:

**Facial Features**
Voice
**Fingerprint**
**Iris**
Retina
Hand Geometry
Signature Dynamics
Keystroke Dynamics
Lip Movement
Thermal Face Image
Thermal Hand Image
Gait
Body Odor
**DNA**
Ear Shape
Finger Geometry
**Palm Print**
Vein Pattern
Foot Print

Desired in all cases:
*uniqueness, acceptance, reliability, low intrusion+cost*

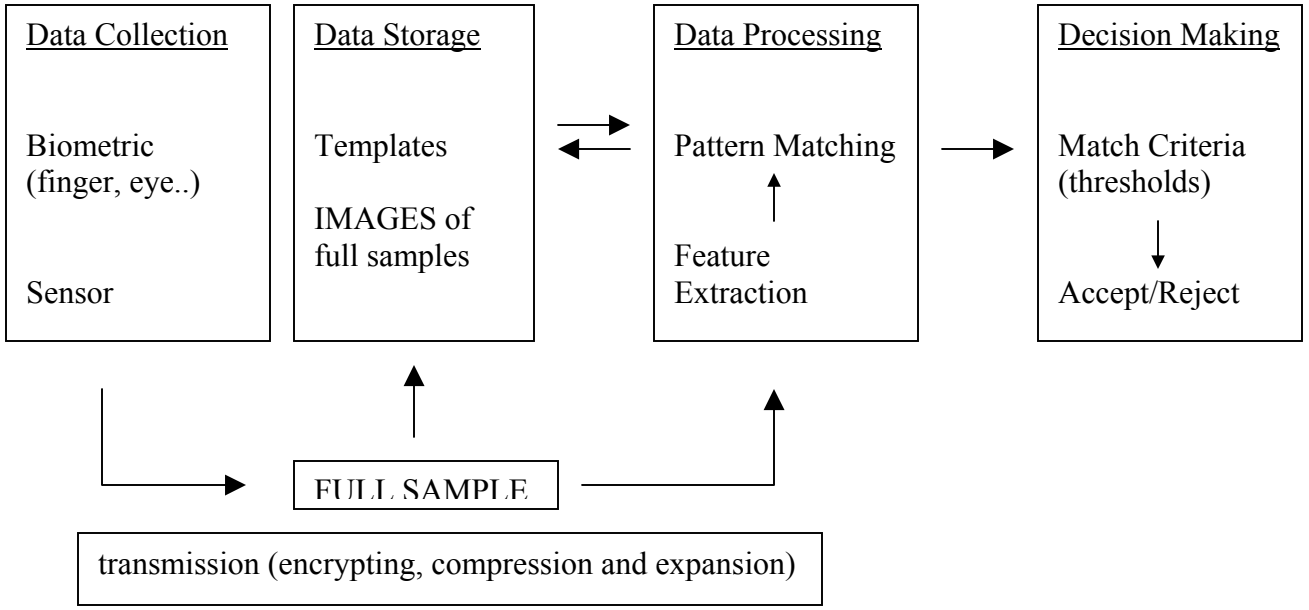



Fig. 3: Diagram of generic biometric system

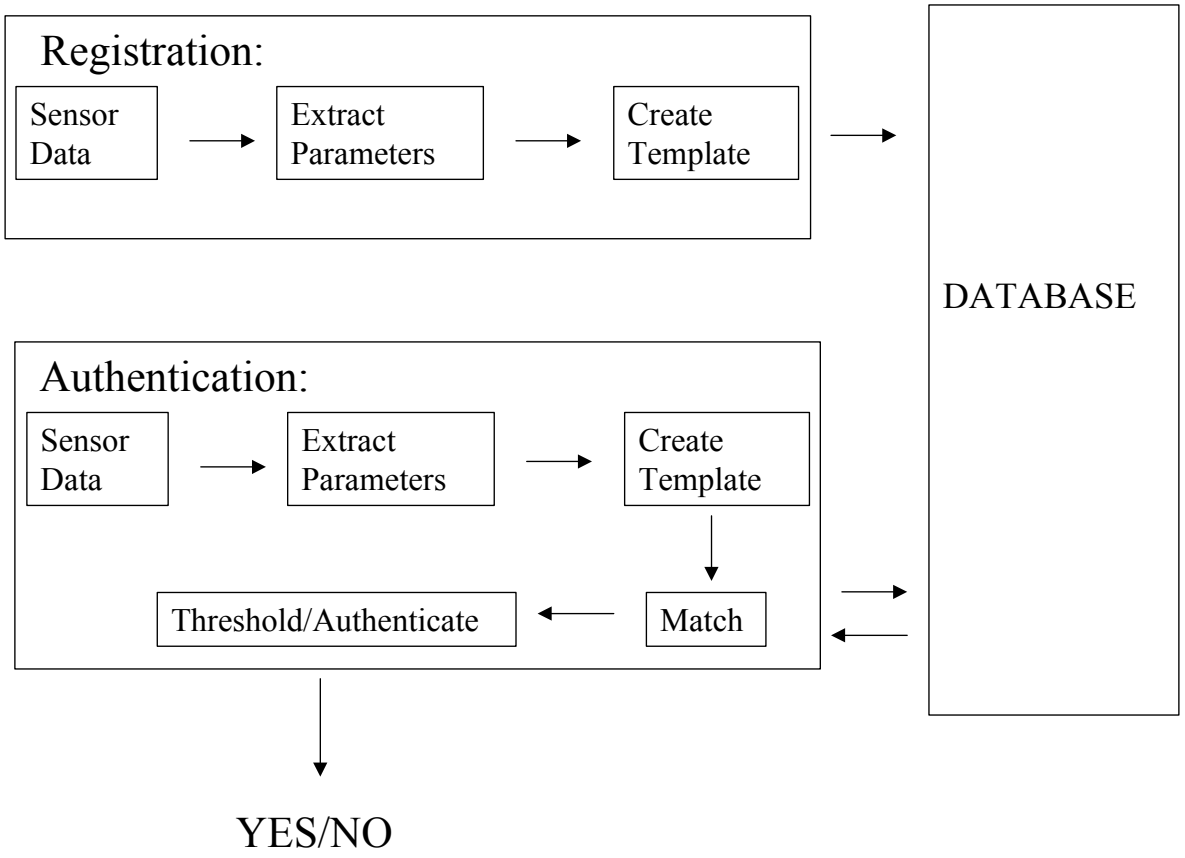



Fig. 4: Diagram of Registration and Authentication processes

# VERIFICATION VS. IDENTIFICATION

- Verification is a *one-to-one* comparison against a single stored template.
- Identification is a *one-to-many* comparison against all the enrolled templates in a database, including N imposters.

Aside:

- If the probability of not getting a false accept is $(1 - P_{fa})$, then the probability of making at least one false accept amongst the N imposters is 1 minus that of not getting a false accept, N times.
- Probability of at least one false accept in identification:

$$\mathbf{P_N = 1 - ( 1 - P_{fa} )^N}$$ where $P_{fa}$ = probability of a false accept in one-to-one verification

- If a biometric verifier achieves a 99.8% Correct Rejection Rate performance in one-to-one verification, then $P_{fa} = 0.002$. When searching through a database of unrelated (imposture) templates the results are:

| Database size | False Accept probability |
|---|---|
| N = 200 | $P_N = 32\%$ |
| N = 2,000 | $P_N = 98\%$ |
| N = 10,000 | $P_N = 99.999\%$ |

- Identification is very much more demanding than verification!
- Make sure is $\mathbf{P_{fa}}$ sufficiently small. If you want 99% certainty that you will not be falsely matched against a database with 10 million templates, then $\mathbf{P_{fa}} = 10^{-9}$: 1 in a billion...

# Decision landscape of biometrics, 1

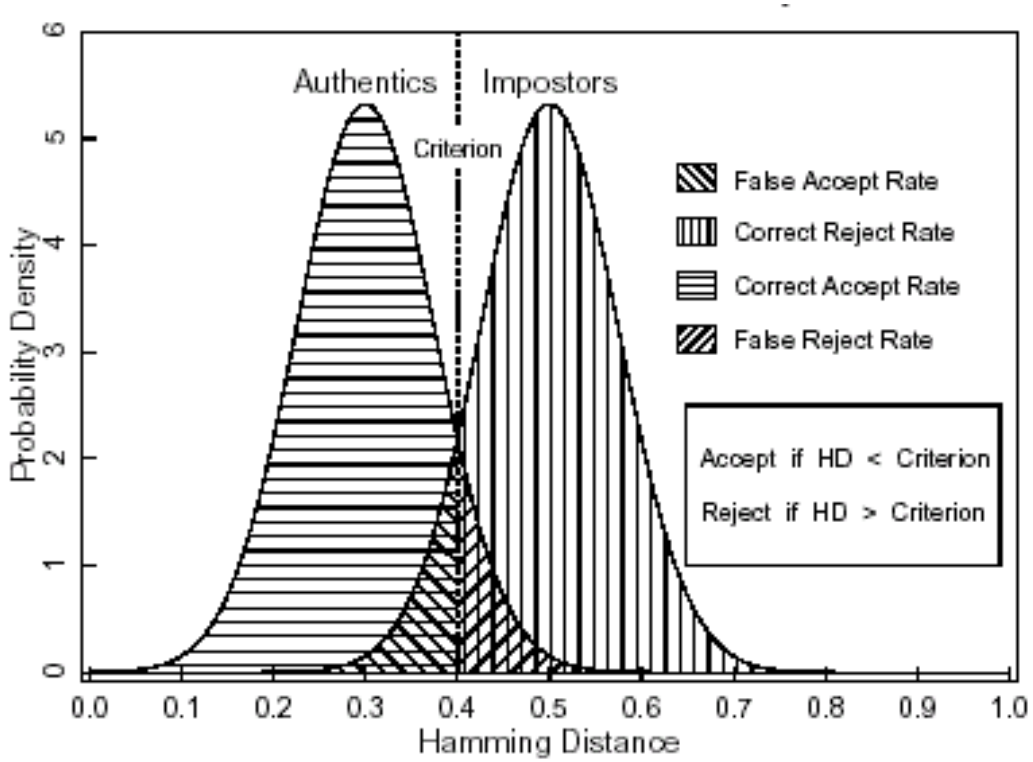



Fig. 5 Decision landscape, Daugman 2000

"Decidability" of a Yes/No decision problem is determined by how much overlap there is between the two distributions. The problem becomes more decidable if their means are further apart, or if their variances are smaller. One measure of decidability, although not the only possible one, is d', defined as follows if the means of the two distributions are μ1 and μ2 and their two standard deviations are σ1 and σ2:

$$d' = |\mu 1 - \mu 2| / ((0.5 * (\sigma_1^2 + \sigma_2^2))^{1/2})$$

# Decision landscape of biometrics, 2

FAR (false acceptance rate)
How often the system falsely recognizes a person who should not be recognized

CAR (correct acceptance rate)
How often the system correctly recognizes a person who should be recognized.

FRR (false rejection rate)
How often the system fails to recognize a person who should be recognized

CRR (correct rejection rate)
How often the system correctly rejects a person who should not be recognized

P(CAR) + P(FRR) = 1
P(FAR) + P(CRR) = 1
P(CAR) > P(FAR)
P(CRR) > P(FRR)

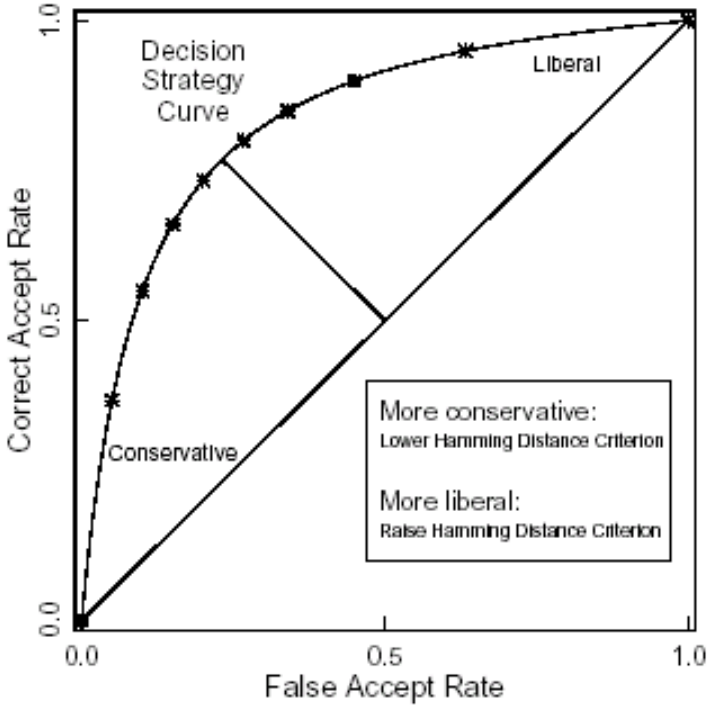



Fig. 6 The Neyman-Pearson decision strategy curve (from Daugman, 2000)

# What is Open Biometrics?

The term is used in different contexts:

- Biometrics for *unstructured systems*, open as in open to unstructured data collections (national ID), as opposed to closed systems, i.e. a counted group of people in a company.

- *Standardized data formats* for compatibility across many computing environments.

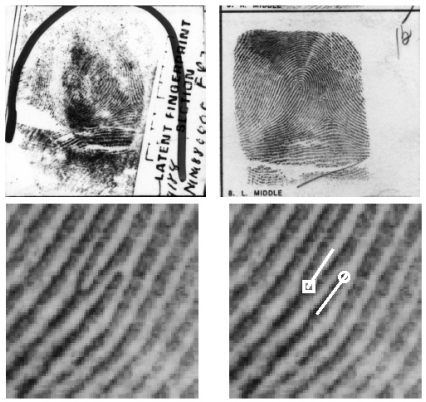
I use the term in this way:

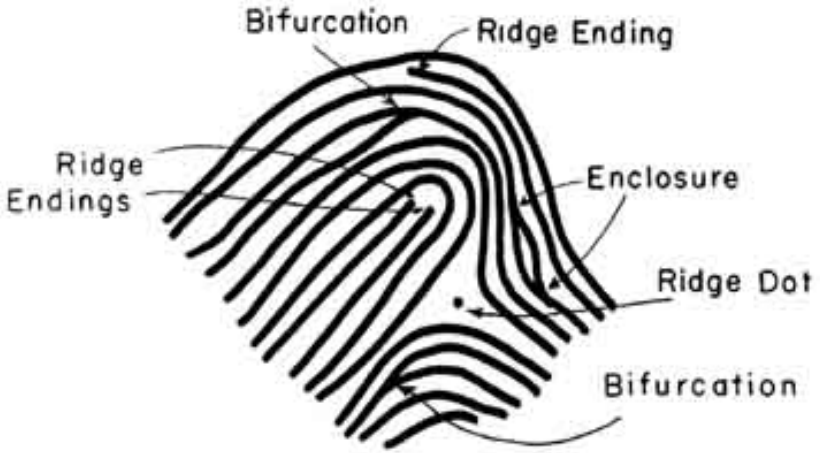
- Open/known assessment criteria, open/known classification procedures and decision thresholds.
  -> *Open decision landscape*
- Open access to your own biometric data. You are the keeper of your own data. You have more of your own data than any other entity (government, institution, etc).
  -> *Open ID card*

# Why is there a need for Open Biometrics ?

- Biometrics are not fool proof.
    - Evidence is often incomplete. In fingerprint analysis partial prints are called *latent* prints.
    - FBI erroneously matched a latent print from the March 11 Madrid terrorist bombing to Brandon Mayfield, recently converted to Islam.
- People define biometrics and people make mistakes, sometime involuntarily.
    - Digital images of insufficient quality are often photoshopped for 'saliency' with no log of changes.
    - Confirmation bias (Mayfield case, 2004).
- Combined Biometrics offer false sense of extra security
    - Multiple biometrics can weaken statistical significance. When two tests are combined, one of the resulting error rates (FAR or FRR) becomes better than the stronger of the two tests, while the other error rate becomes worse even than the weaker of the two tests (Daugman 2000).
- Grand scale plans to introduce biometrics registration on national and international levels.
    - UK's national identity card scheme
- General belief in biometrics as a panacea against all ills (immigrants, illegal works, terrorists, etc).
    - 79% of the opportunistic category of participants in the UKPS Biometrics Enrolment Trial believed biometrics would help prevent illegal immigration.

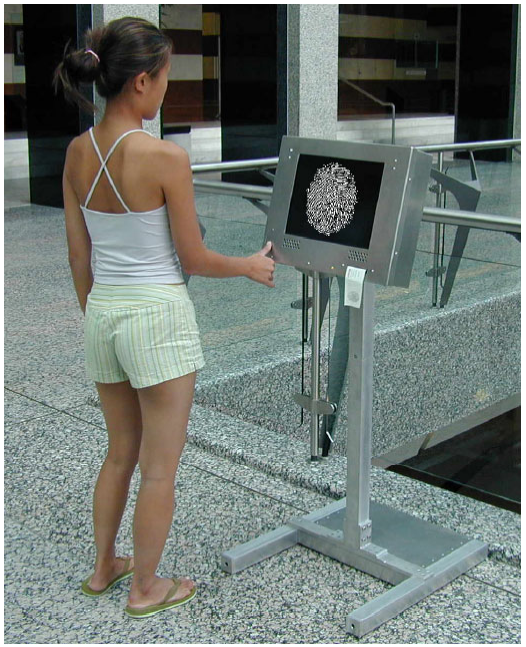
arch and whorl






Pattern and minutiae based data

Fig. 7 fingerprints and features

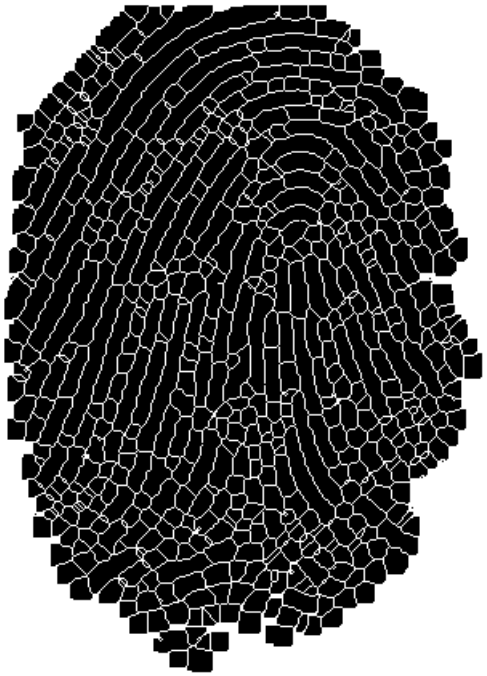

Approach:

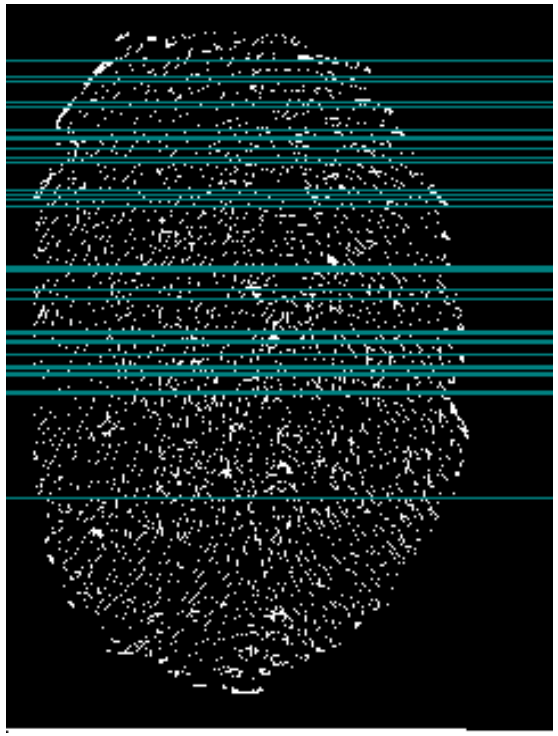
1) Do not reduce the data to a representative (convenient) subset:

- Show all data (do not threshold the results)

- List the probabilities.

Fig. 8 fingerprints and open listing of probabilistic minutiae





Approach:

2) Require data deletion.

-Do not keep records a system does not need.

-Prevent data collection creep

```
If(Endday)
{
        for each m:
        OData[m] = EthPath + OData[m] ;
        remove(OData[m]);
}
```

Fig. 9 data deletion

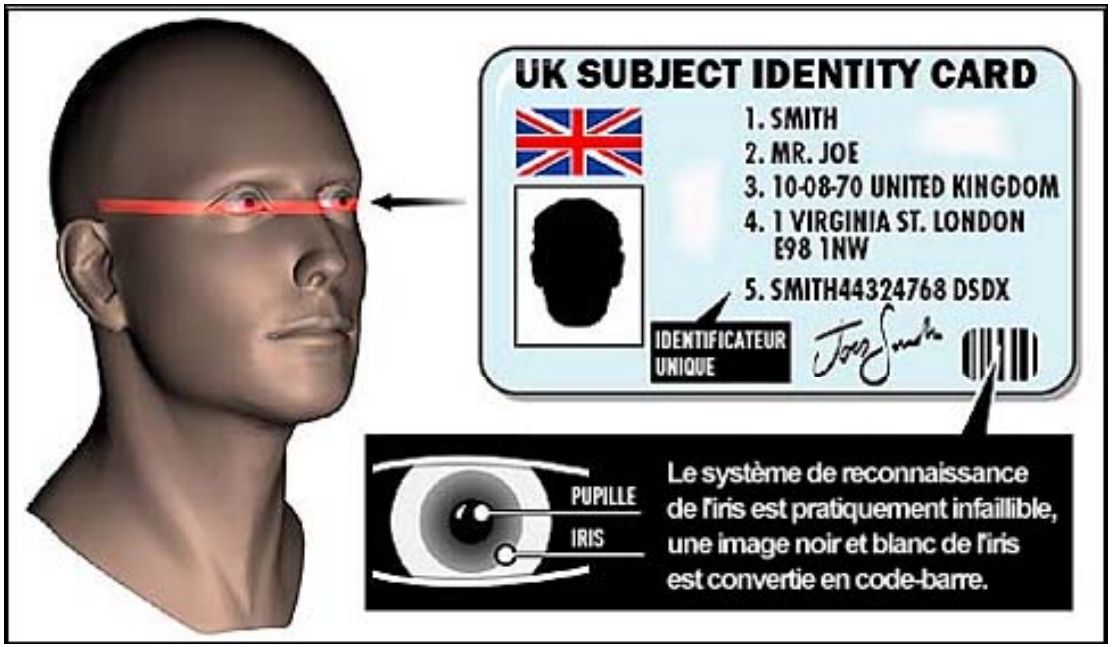



Fig. 10 UK Subject Identity Card

Fig. 11 UK Mobile Enrollment Unit

UK Passport Service Biometrics Enrolment Trial 2004:
Enrollment and verification for facial, iris, finger print biometric, and 'customer experience'.

- The three sample groups (total 10.016).
- Quota sample of 2,000, matching UK population,
- Opportunistic sample of 7,266, no demographic factors included ('off the street'),
- Disabled participant sample of 750 (Atos Report May 2005)

# Open Biometrics, Version 2, Combined Large Scale Biometrics

**NISTIR 6529-A**

## Common Biometric Exchange Formats Framework

### 1 Scope

NISTIR 6529-A specifies a common set of data elements necessary to support multiple biometric technologies and to promote interoperability of biometric-based application programs and systems by allowing for biometric data exchange. These common data elements can be placed in a single file, record, or data object used to exchange biometric information between different system components and applications. This publication specifies the Biometric data elements. These elements are assembled into data structures that are defined by CBEFF Patron Format Specifications or standards. Each CBEFF-compliant Patron Format Specification defines which CBEFF data elements are present in its format and how the data elements are extracted and processed (details such as the data encoding scheme are the responsibility of the CBEFF Patrons). The Biometric data elements transported in a CBEFF structure can represent processed or unprocessed (raw) data.

CBEFF does not specify the content or format of the actual biometric data contained within a CBEFF biometric data record.

Protection of the privacy of individuals from inappropriate dissemination and use of biometric data is not in the Scope of this NISTIR.

### 2 Conformance

From: NISTIR 6529-A, National Institute of Standards and Technology, Technology Administration, US Department of Commerce, April 2004

# Need for checks and balances in large-scale biometrics: WORLD CARD

## CARDS

- Every country receives the technology to create WORLD CARDS and makes them available for a modest fee to their citizenry

## DATA

- Individuals hold the most complete set of (biometric) data of themselves in universally accepted formats.
- Data must be high quality, raw, without digital modifications.

## DECISION METRICS

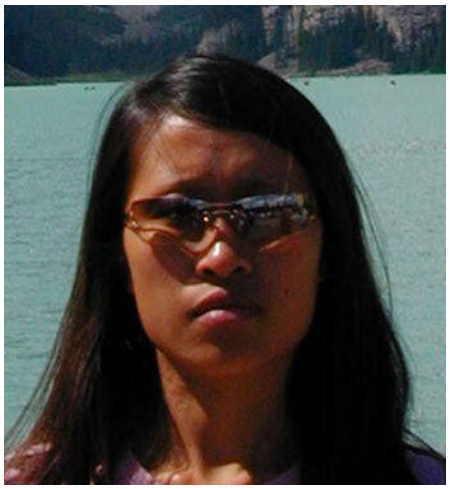
- Decision metrics must be made known and set in accordance with World Card standards.
- Results must include probabilistic data.

## INTERNATIONAL LAW

- Law enforcement and legal courts are required to reference WORLD CARD when making biometrics based identification
- WORLD CARD based proof of identity hold precedence over all other forms of biometric based identification.

# WORLD CARD

| | |
|---|---|
| NAME: | JANE TAN |
| ISSUE DATE: | 13. July 2005 |
| VALIDITY PERIOD: | 13. July 2005 to 12. July 2010 |
| BIOMETRIC PURPOSE: | Reference Identification |
| CREATOR: | UNITED NATIONS |
| BIOMETRIC TYPES | Iris, Finger, Hand, Gait, Grip, Odor |
| BIOMETRIC SUBTYPE: | Iris, right eye |
| BIOMETRIC DATA BLOCK | 5689 7867 |
| BIOMETRIC SUBTYPE: | Thumb, left hand |
| BIOMETRIC DATA BLOCK | 7888 3367 |
| BIOMETRIC SUBTYPE: | Hand, left hand |
| BIOMETRIC DATA BLOCK | A787 3454 |
| BIOMETRIC SUBTYPE: | Gait, walking |
| BIOMETRIC DATA BLOCK | 1255 6A77 |
| BIOMETRIC SUBTYPE: | Grip, dynamic |
| BIOMETRIC DATA BLOCK | 4509 5T33 |
| BIOMETRIC SUBTYPE: | Odor, mouth |
| BIOMETRIC DATA BLOCK | 1201 2A66 |



5689 7867IKGHEKAJ
7888 3367GJAHEIET
A7873454KHJ594YI1
12556A77HKJIUYU4
5095T3357665HKJL1
2012A66MUIOY89G

*As per United Nations stipulations, biometric identification must occur with reference the data contained in this card in order to be upheld in any United Nations accepted court of law. Only the data on this card and the corresponding decision metrics are acceptable for proof of physical identity.*

Fig. 12 World Card template

| | |
|---|---|
| BIOMETRIC DATA QUALITY | 100 |
| BIOMETRIC DATA TYPE | RAW |
| BIOMETRIC DATA SIZE | 2048 bits |
| BIOMETRIC CREATION | Gabor wavelet base phase demodulation for pseudo-polar coordinate system where the real and imaginary parts define the positive and negative bits of iris code. |
| DECISION METRIC | modified Hamming distance |
| DECISION THRESHOLDS | 14.0 |

Very Short Bibliography:


- “Feasibility Study on the Use of Biometrics in an Entitlement Scheme:, Mansfield and Rejman-Greene, 2003
  http://www.homeoffice.gov.uk/docs2/feasibility_study031111_v2.pdf
- “Best Practices in Testing and Reporting Performance of Biometric Devices”, Mansfield and Wayne, 2002
  http://www.npl.co.uk/scientific_software/publications/biometrics/bestprac_v2_1.pdf
- “Biometrics Enrollment Trial Report” Atos Origin, 2005
  http://www.passport.gov.uk/downloads/UKPSBiometrics_Enrolment_Trial_Report.pdf
- “Lessons From The Brandon Mayfield Case”, Thompson and Cole, National Association of Criminal Defense Lawyers: Forensics, 2005
  http://www.nacdl.org/public.nsf/0/3419bfeee2f5c72c85256ff600528500?OpenDocument
- NISTIR 6529-A, "Common Biometric Exchange Formats Framework (CBEFF)", 2004:
  http://www.itl.nist.gov/div893/biometrics/documents/NISTIR6529A.pdf
- "Biometric decision landscapes." Daugman, Technical Report No. TR482, University of Cambridge Computer Laboratory, 2000.
  http://www.cl.cam.ac.uk/TechReports/UCAM-CL-TR-482.pdf
- “Digitized Prints can Point Finger at the Innocent”, Chicago Tribune, Flynn McRoberts and Steve Mills Tribune staff reporters January 3, 2005
  http://www.truthinjustice.org/digitized-prints.htm


Some Institutes:

- NPL: National Physical Laboratory (UK)
  http://www.npl.co.uk/scientific_software/research/biometrics/
- Cambridge University, Computer Laboratory (UK)
  http://www.cl.cam.ac.uk/users/jgd1000/
- NIST: National Institute of Standards and Technology (USA)
  http://www.itl.nist.gov/
- Biometric Systems Lab, U. Bologna (ITALY)
  http://bias.csr.unibo.it/research/biolab/bio_tree.html

Other Sources:

- Biometrics Consortium: link between government and industry
  http://www.biometrics.org/
- Michelle Triplett's fingerprint terms
  http://www.fprints.nwlean.net/e.htm
- Crypto-Gram Newsletter, Bruce Schneider
  http://www.schneier.com/crypto-gram-0404.html