Technical Aspects of the National Identity Card

Nigel Sedgwick

Cambridge Algorithmica Limited
9 Oakdene
Beaconsfield
Buckinghamshire
United Kingdom HP9 2BZ

Tel: +44 (0)1494 678989
URL: http://www.camalg.co.uk
Fax: +44 (0)1494 678990
Email: ncs@camalg.co.uk

Overview of Presentation

1. Functions of the National Identity Scheme (NIdS)
2. General Aspects of Biometrics
3. Performance Measures for Biometrics
4. Biometric Modalities expected in the NIdS
5. Likely Performance Requirements for the NIdS
6. The Contribution of Multi-Biometric Fusion
7. Security Vulnerabilities with NIdS Biometrics
8. Civil Liberties Considerations
9. Cost Effectiveness Aspects
10. Summary of Issues Presented

Primary Functions of the NIdS Biometric Component

Verification: of the identity of a previously registered person, using biometric matching against template(s) of the claimed identity. This is useful where a person wishes to have their identity confirmed.

Detection of Multiple Applications: at initial registration and biometric enrolment, using biometric matching against templates of (potentially) all persons already registered. This is to reduce the availability of false identities used for criminal purposes.

Identification: of whether a person is registered and which registered person they are, using biometric matching against templates of many or selected enrolled persons. This is useful where, for example, an arrested person refuses to cooperate with the police concerning their identification, or a foreign person claims to the police not to be a resident and this is doubted.

Technical Components of the NIdS Relevant to Identification Security

Biometric Enrolment and Matching: Identification by biometrics is statistical in nature, with a lack of certainty greater than is understood by many people. Biometric performance is key to NIdS effectiveness.

Digital Signatures: These provide protection against forged identity cards, with partial substitution of data.

Encryption of Communications: for protection against eavesdropping and injection of falsified or copied data.

IT Security: the whole range of techniques is appropriate for protection against illegal access and modification of stored data) and of modification of computer programs, on the NIR, PoU computers and any on-token processors.

Hardware Tamper Detection: particularly for biometric devices, matching computers, etc at Points-of-Use (PoUs).

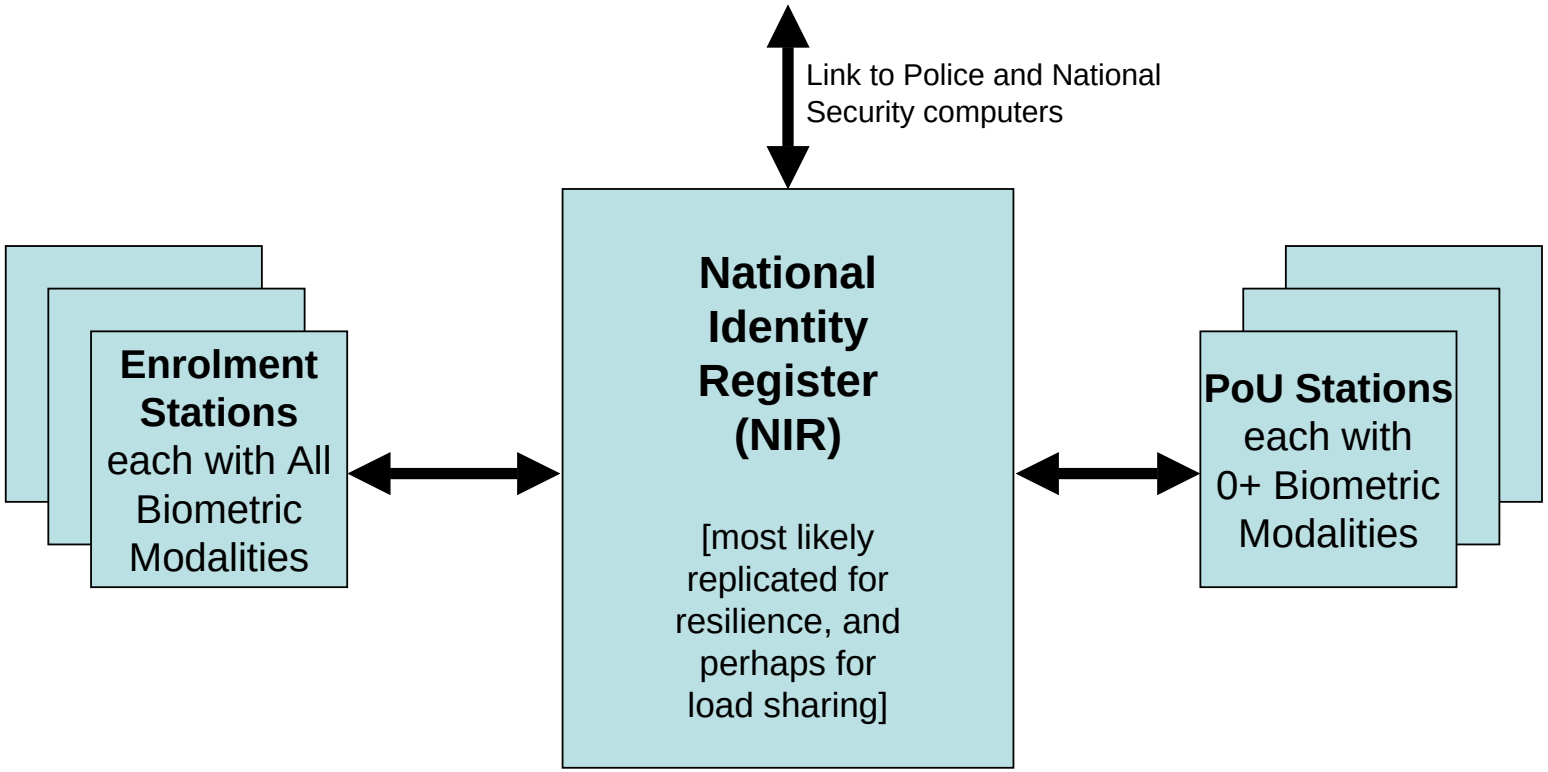
Secondary Functions of the NIdS Biometric Component

Watchlist Preparation: primarily as a source of templates for registered persons who have been placed on one or more watchlists. Watchlists are used to determine the passing by or through of selected persons. This would be particularly if they were suspected of using false identities, or if no overt identity checks were being made at the watch points.

Forensic Checks: by matching scene-of-crime (SoC) evidence, particularly latent fingerprints, against all, many or selected biometric templates of registered persons.

Note: Both of these actions would most likely be done without permission or cooperation of the subject; in some cases at least, also without them knowing. The Government has stated that these secondary functions would usually concern persons under investigation for suspected serious criminal activity, or for national security purposes.

Biometric Components of the NIdS



Access Constraints to the NIR

Point-of-Use (POU) Stations: No download access (major security feature). Upload some identity details (eg Identity Registration Number (IRN), name, address) and biometric sample(s).

The NIR reports only two result types, just as TRUE/FALSE:

(i) name/text details etc match an NIR record;
(ii) biometric sample(s) match specified NIR record.

Enrolment Stations: Can download, edit and upload identity details, photographs, etc and upload biometric samples/templates. Can instruct NIR on Detection of Multiple Applications, and download detailed results for secondary checks.

Police & National Security Access: Can download name, text details, etc and upload biometric samples. With authorisation, can instruct NIR on 1:N matching for identification of uncooperative persons, and download biometric samples/templates for watchlists and forensic checks. Can request update of identity details.

Identity Checking Options at PoU (1)

Points of Use: Many throughout the country, for government, commercial and other uses. All PoUs need prior authorisation to access the NIdS, most likely including formal registration and receipt of crypto keys.

Access Permission from Registered Person: This is assumed to be required, and implicitly given by presenting the card or by giving some identity details (eg name, address).

Anyone Without Formal PoU Registration can use:

Manual Inspection of ID Cards: Printed details are available for all to inspect, including name and photograph; likely to also include address and IRN.

Identity Checking Options at PoU (2)

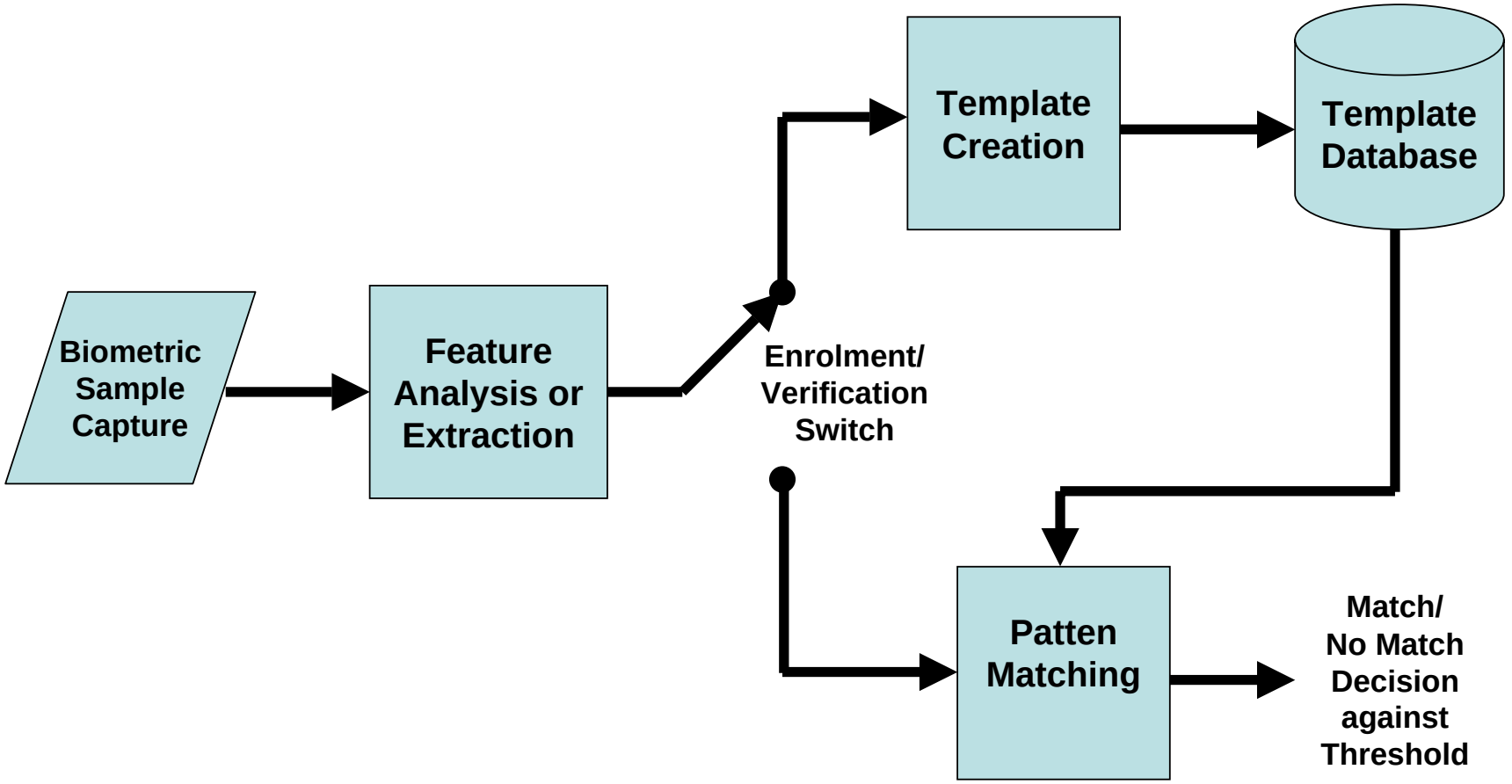
With Formal PoU Registration can do:

Off-line Check of Data Content of ID Cards: Card reader accesses and displays on-card digital data. Digital signature protects against forgery or data substitution. Digitised photograph and other details from card can be checked on PoU station display.

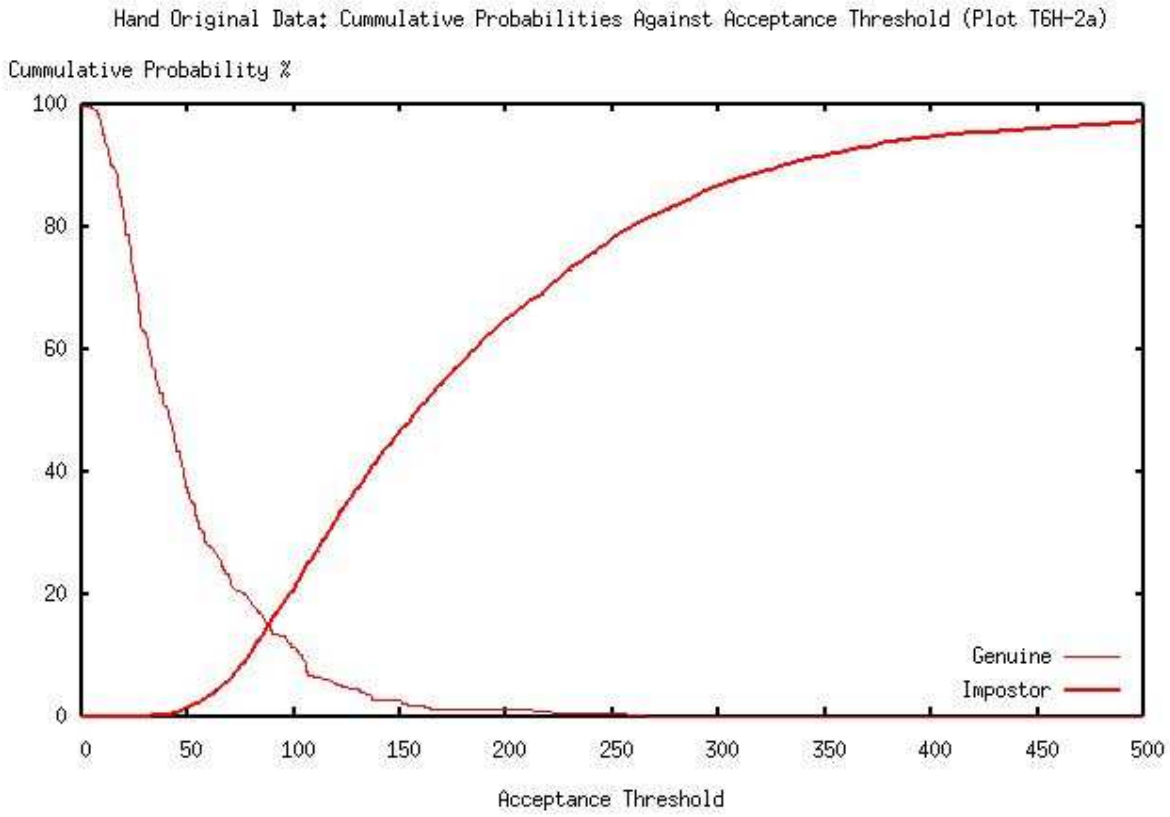
Off-line Biometric Check: Card reader accesses on-card biometric template(s); station matches against these against biometric sample(s) from cardholder.

On-line Data and/or Biometric Checks: Requires on-line access. Can be done if cardholder has not got card with him/her. On-line verification can use more and different biometric templates than on card, for greater reliability of identification. On-line access causes entry into NIR Audit Trail.

Generic Structure of a Biometric System



Plots of FNMR and FMR against Score

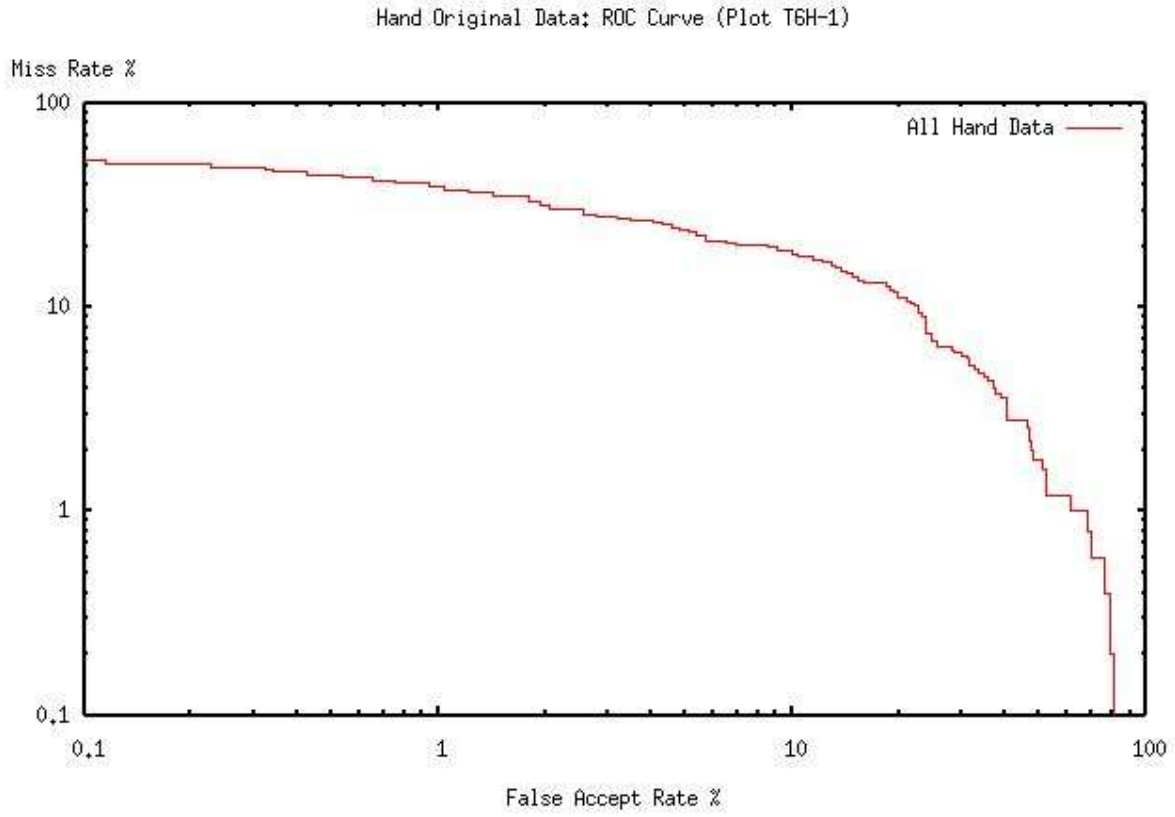


FNMR: False Non-Match Rate (Verification Miss Rate)

FMR: False Match Rate (Verification False Alarm Rate)

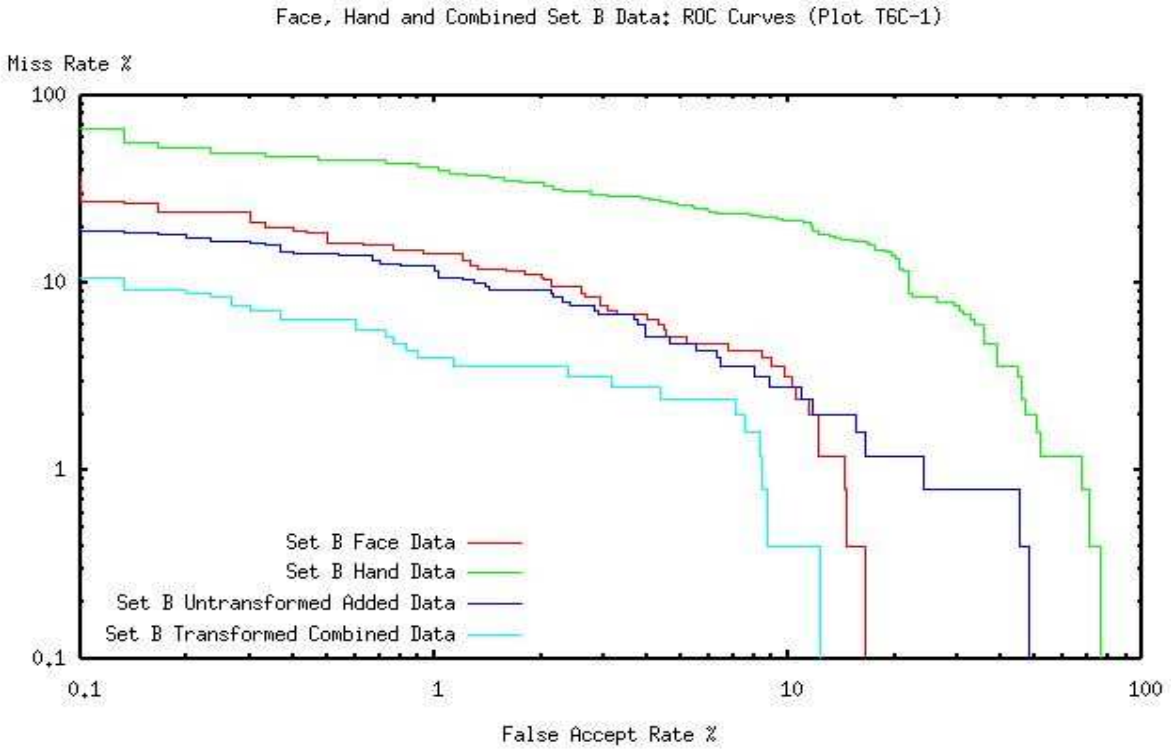
EER: Equal Error Rate (FMR==FNMR)

Receiver Operating Characteristic (ROC) Curve



Best plotted on a log-log scale, to give wide dynamic range.
Also known as the Detection/Error Trade-Off (DET) Curve.

ROC Curve Comparison of 2+ Biometrics



Plots of whole ROC curves are necessary to determine which biometric is best at each operating point (acceptance threshold). Sometimes ROC curves cross, such that one biometric is better at some thresholds, and another is better at other thresholds.

Performance Measures for Biometrics

ROC Curve: This is the main performance measure.

FNMR/FMR at a particular operating point: Note that both rates must be given, to be meaningful. Sometimes given at several operating points (eg FNMR at FMR of: 0.01%, 0.1%, 1%). The Equal Error Rate (EER) can be used as an approximate "single figure of merit".

Failure to Enrol (FTE) Rate: This is usually indicative of the proportion of the population who cannot use a particular biometric, because of missing, damaged or aged body parts.

Failure to Capture (FTC) Rate: This is usually indicative of the ease of use of a particular biometric device.

Use of Multiple Capture Attempts (Multi-Presentation): Repeats are usually allowed, say of up to 3 capture attempts. The above performance measures are often quoted after allowing repeats, using the best scoring attempt of those given.

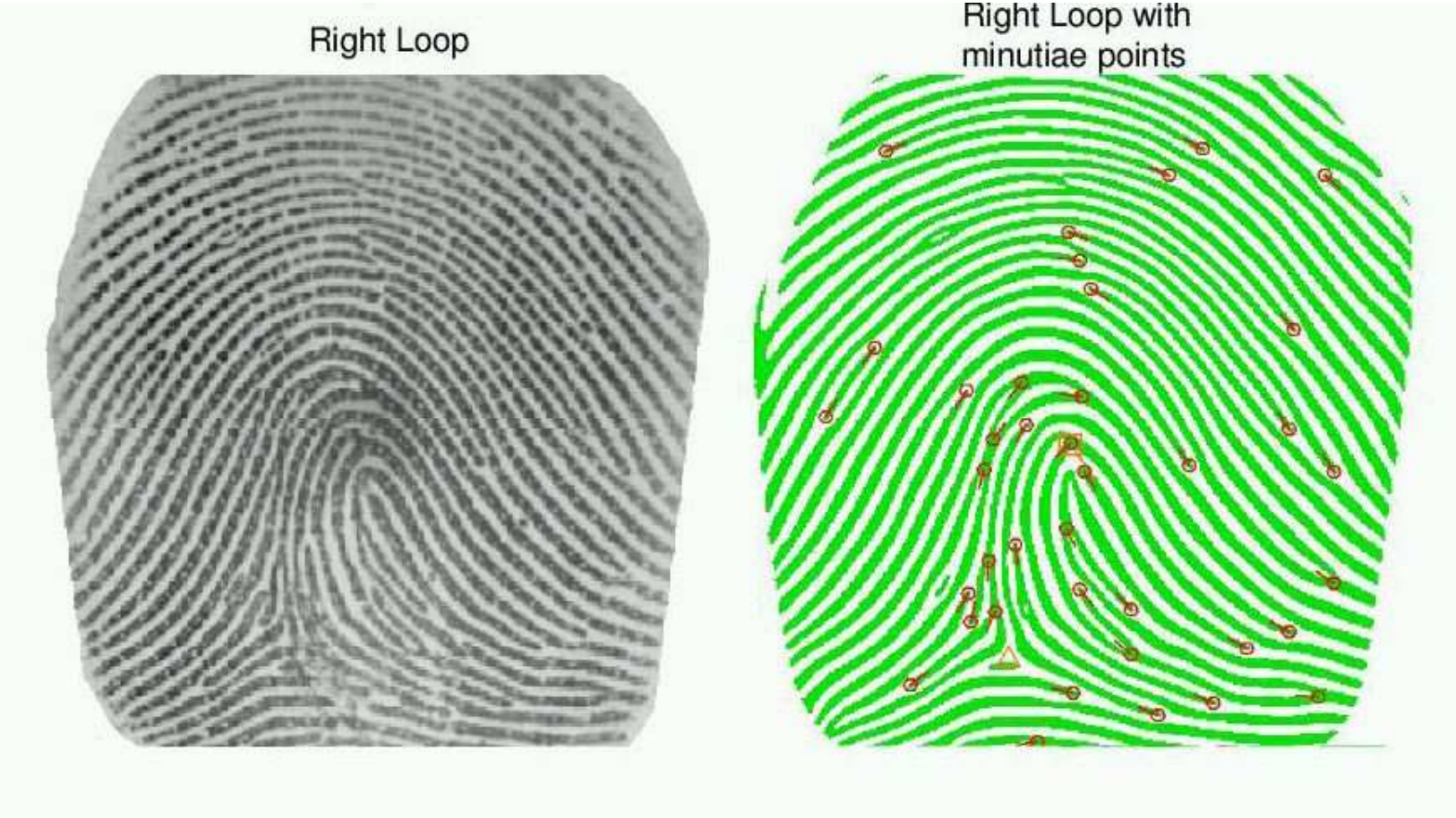
Modalities Likely to Feature in the NIdS

Fingerprint: Well known and understood from use in scene-of-crime forensics, with computerised Automatic Fingerprint Identification Systems (AFIS). Low cost sensors available. Good identification performance, especially with multiple-instances.

Iris: The best matching algorithms (Daugman, 1993) are now a bit past their tenth birthday and the technology has become widely accepted. Very good identification performance, though some difficulties with ease of use. Despite concerns expressed, there are no material health risks.

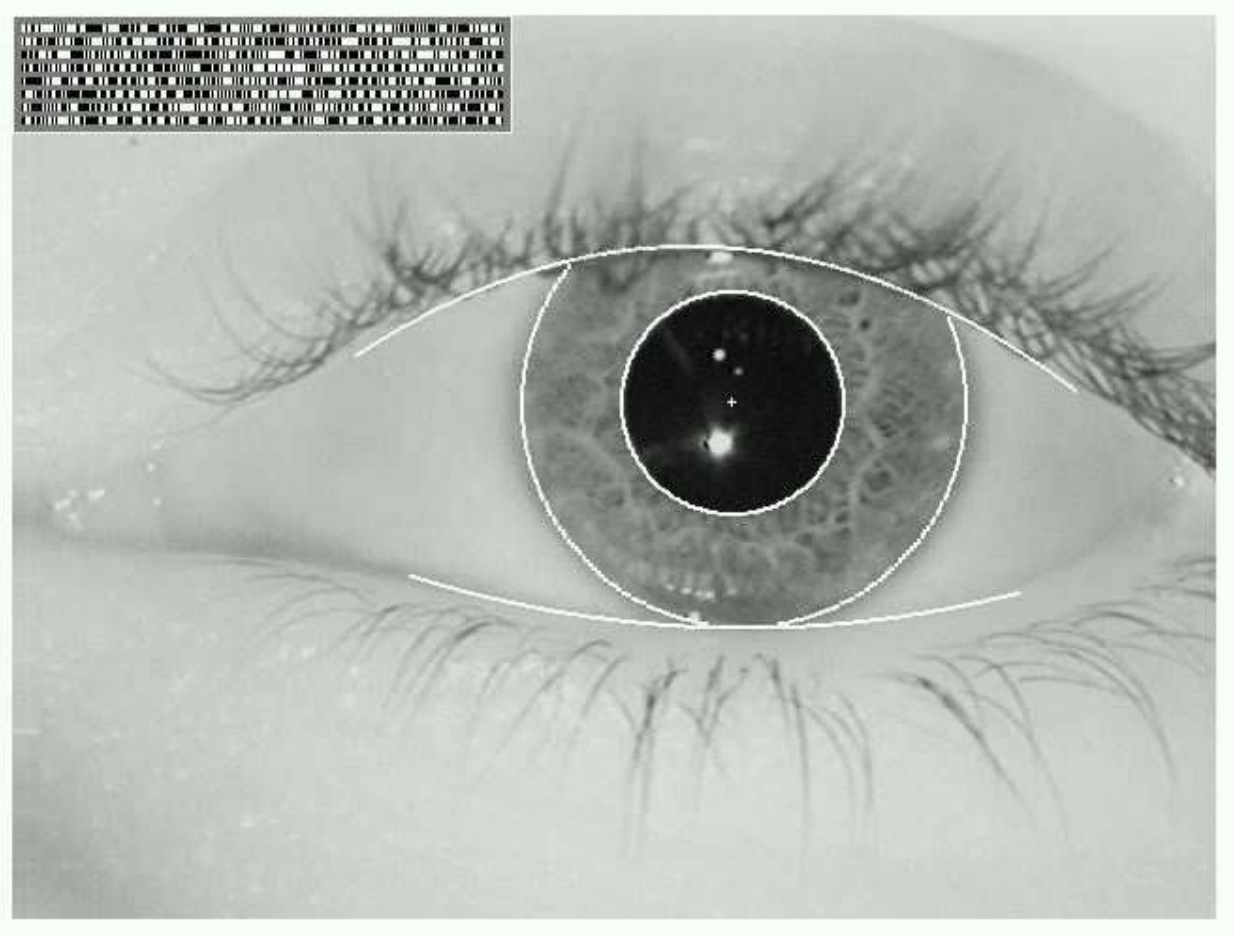
Face: Well known, with low cost sensor (CCTV camera) and possible enrolment from photographs. Recognition performance is not very good, though ease of use and acceptability are usually rated as high.

Example of Fingerprint Biometric Sample



Reproduced with permission from: "An evaluation of fingerprint image quality across an elderly population vis-Ã -vis an 18-25 year old population", Nathan Sickler and Stephen J. Elliott, IEEE International Carnahan Conference On Security Technology, Las Palmas De Gran Canaria, Spain, 2005:
http://www.carnahan2005.ulpgc.es/programme/presentaciones_pdf/12_Miercoles/2a/2.-Sickler%20Carnahan%202005%20Presentation.pdf

Example of Iris Biometric Sample



Reproduced with permission from Professor John Daugman of the Cambridge University Computer Laboratory: http://www.cl.cam.ac.uk/users/jgd1000/iriscode.jpg

Specifying Biometric System Performance Requirements in General

A very difficult task: In theory, we can analyse the issue in terms of Bayesian risk, using *a priori* probabilities of the subject being genuine, the FNMR/FMR at each operating point, and the cost of the two types of error; this allows us to determine the optimum operating point, or an acceptable one to strive for with our biometric technology. However, in practice, most of the necessary values are not known well enough.

Asset Value: What is the value of "identity" to its legitimate owner, and to attackers? It depends very much on the circumstances.

***A Priori* Probabilities**: What is the probability, before any biometric checks, that the subject is the genuine cardholder?

Deterrent Effect: This depends on the attackers' perceptions (rather than the actuality) of the chances of being detected and apprehended, and on the expected punishment (eg prison).

Performance Requirements for NIdS Verification; an Example

Bankers Draft for £100,000: One must weigh the issues of "insulting" the bank's customer with over-zealous checking, against the risk to the bank of losing its money. Perhaps an *a posteriori* average risk of £10 is acceptable. That requires a 0.01% *a* posteriori probability of an impostor; if the *a priori* risk of an attempted fraud is 1%, the biometric identity check must improve this by a factor of 100 (the BGI: Biometric Gain against Impostors), which determines the acceptance threshold. However, we also need the FNMR to be low enough to avoid irritating too many customers; perhaps a 2% rate is tolerable. Is our biometric device good enough to provide this?

Bankers' Draft for £250,000: To be logical about this, the acceptance threshold should be different from the £100K case.

Customer Expectations: Some customers are more easily irritated than others; the bank may value some customers more than others.

Performance Requirements for Detection of Multiple Applications

There is a desire to prevent multiple applications passing undetected, even after say 40 million people have already enrolled.

Each false match needs to be checked by non-biometric means. For extra checks on only every 10th applicant, the FMR needs to be around 0.00000025% ($2.5x10^{-7}$%).

What proportion of undetected duplicate applications is acceptable? Do we need 95% detection, or 99%, to be a good enough deterrent. Or perhaps even better against terrorist commanders. This determines the tolerable FNMR.

An operating point with 1% FNMR and 0.00000025% FMR is about equivalent to an Equal Error Rate (EER) of 0.0005%.

What is Multi-Modal Combination?

Using 2 or more different biometric modalities, together, in deciding whether the subject is genuine or an impostor.

Examples are: iris combined with fingerprint; face combined with hand geometry.

*Other **Multi-Biometric** vocabulary terms include:*

multi-instance: **combining more than one separate instance of the same biometric modality; eg fingerprints from 2 or more different fingers**

multi-algorithmic: **processing the same biometric sample with 2 or more pattern-matching algorithms, and combining the results**

multiple presentation: **capturing the same biometric instance (eg a single fingerprint) more than once, to reduce image capture errors; usually the best scoring presentation is used**

Benefits of Multi-Modal Combination

Improved Technical Performance, in terms of a better trade-off between False Match Rate (FMR) and False Non-Match Rate (FNMR).

Greater Universality. A greater proportion of the population of subjects will be able (and willing) to present examples of at least one of the biometric modalities. For example, those with poor quality fingerprints, amputated body parts, etc could still offer one or more alternative biometric modalities.

Greater Resistance to Biometric Avoidance Techniques. Impostors need to spoof more than one biometric device at the same time; eg gelatine false fingertips.

Other multi-biometric techniques, eg multi-instance and multi-algorithmic, also provide some of the above advantages.

Downside Issues with Multi-Modal

Capture requires multiple biometric devices, with associated procurement and maintenance costs.

Enrolment is likely to take longer, for subjects.

Longer enrolment increases costs of any supervising staff.

Multi-modal verification, if done, has similar cost issues and response time issues.

Multi-modal combination needs extra processing. Device characterisation requires pre-operational work; the verification computational load of fusion is much less problematic.

Templates have to be stored for each biometric modality.

Biometric Gain: the Concept (1)

It's rather like hi-fi amplifier gain; one just considers the ratio of the output to the input, of each biometric subsystem.

For verification, we use the Biometric Gain against Impostors (BGI).

$$\text{BGI} = \frac{\text{Probability of being an impostor, given the biometric evidence too}}{\text{Probability of being an impostor, given only prior knowledge}}$$

Most of the time, a very good approximation to the BGI is the Likelihood Ratio of Genuine to Impostor (LRGI). **This is used in many good pattern-matching algorithms in existing biometric subsystems.**

$$\text{BGI} \simeq \text{LRGI} = \frac{\text{Probability of seeing the evidence from an impostor}}{\text{Probability of seeing it from the expected genuine subject}}$$

Biometric Gain: the Concept (2)

Score Normalisation: Every score that comes out of the biometric devices is transformed to the LRGI scale. It can be done within each biometric subsystem, or by a special multi-biometric fusion subsystem.:

We do not need *a priori* probabilities for multi-biometric fusion using LRGIs.

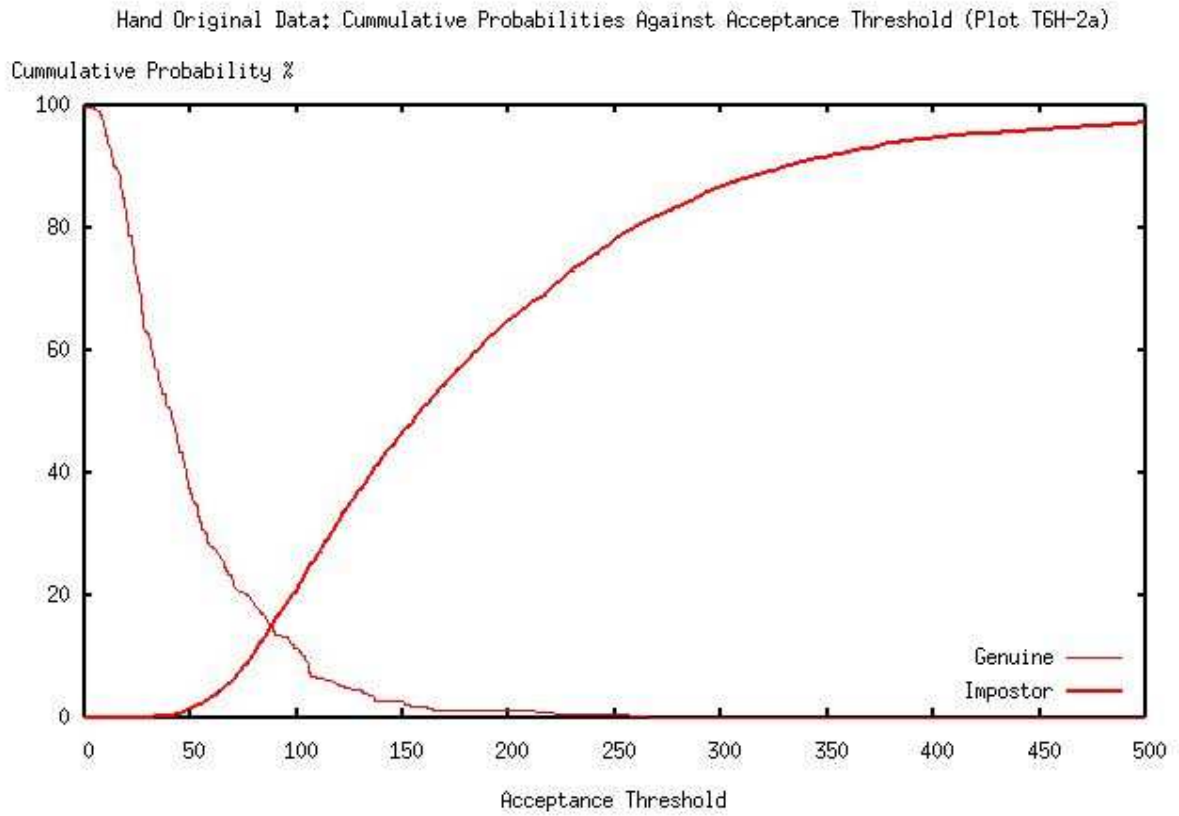
LRGI Normalisation Advantage: Takes account of the intrinsic FMR/FNMR performance of each biometric device, irrespective of operating point, as well as taking account of the score of the particular match.

LRGIs can be combined by multiplication: or by adding log likelihood ratios, which has dynamic range advantages. This works quite well even with correlated scores (eg multi-algorithmic).

For some applications, the acceptance threshold can be set on the LRGI scale, without needing to know the *a priori* probabilities

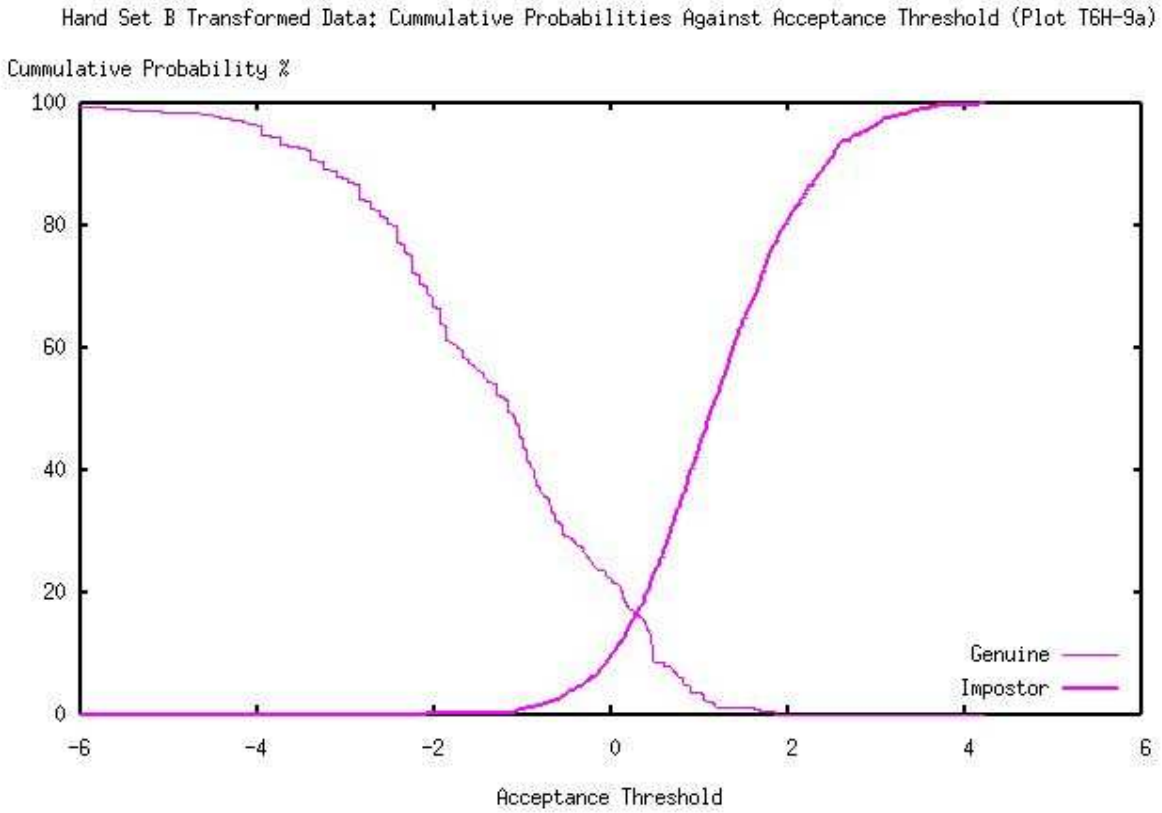
Score Normalisation: What it Does (1)

Plot of FNMR (genuine) and FMR (impostor) against unnormalised scores, for hand geometry subsystem. Note EER of 16.6%.



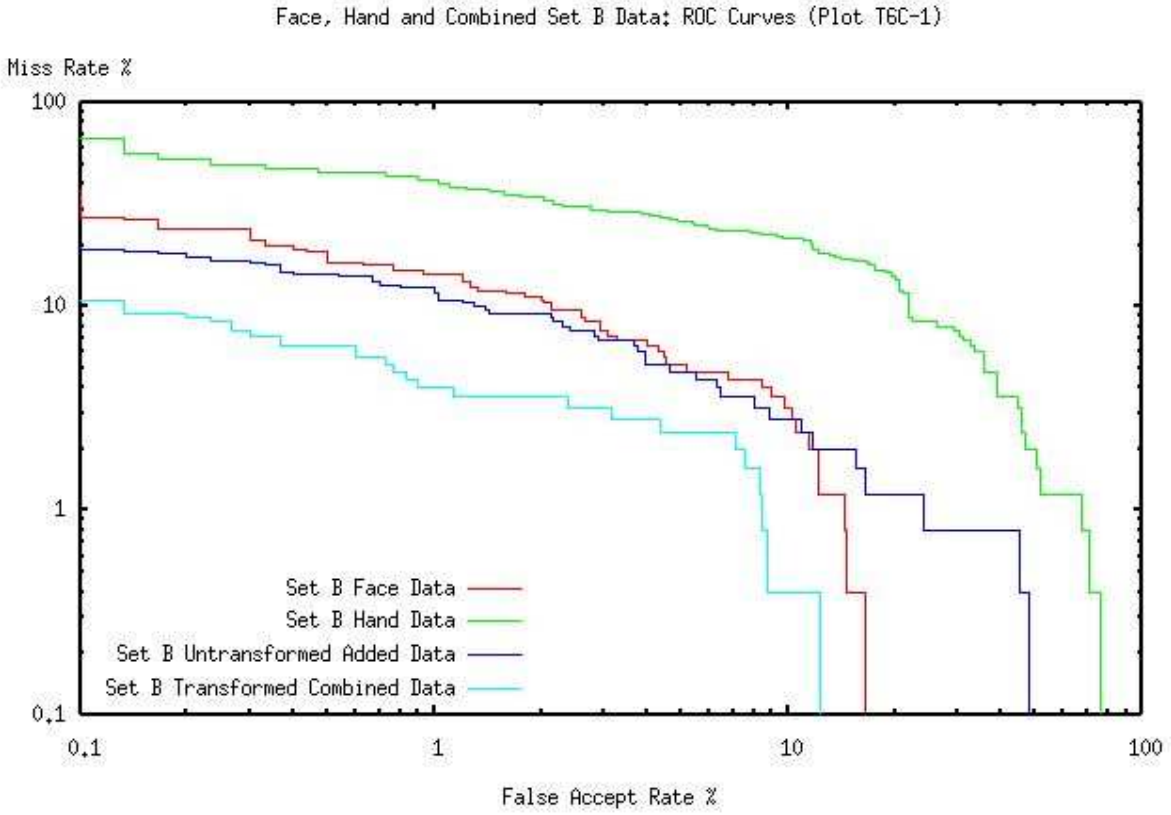
Score Normalisation: What it Does (2)

Same data for FNMR (genuine) and FMR (impostor), but plotted after score normalisation to log(LRGI). Note the unchanged EER of 16.6%.



Example Performance (3): Combination by Biometric Gain does Better

The BGI combination (light blue) gives a good improvement over the whole range of operating thresholds. BGI also does better than just adding the unnormalised scores (dark blue).



Security Vulnerabilities with Biometrics

Forged ID Cards: Protect against this and substituted data with digital signatures. This protection is advantageous, even without biometrics, with manual checks on digitised photographs.

Recording/Re-Injecting Data in Transit: Protect with encrypted communications. Distribution/protection of crypto keys is an issue, especially with PoU computers without physical protection at all times. Tamper detection plus good operational procedures offer some protection; however, this is anathema to many computer users.

Artefact Attacks: Copy template from ID card or elsewhere, or copy biometric from person (eg fingerprint on card or on beer glass in pub) and use artificial means to attach/overlay a copy on the infiltrator's biometric instance (gummy fingerprint; contact lens).

Infiltrator Selection : Again copy template biometric. Select person in band of conspirators whose own biometric matches adequately to that of the target. Also, obtain all biometric templates from NIR and chose target to match well to biometric instance of chosen infiltrator.

Architectural Issues for NIdS

Match on Central System: Avoids risks from exposure of biometric templates on identity cards. However, requires continuous availability of on-line access to central NIR System.

Template on Card / Match on Station: Avoids need for on-line access to NIR. However, exposes biometric templates on lost/stolen/cloned cards to artefact attack and infiltrator selection.

Match on Card: Avoids exposure of biometric templates on cards, by ensuring templates never leave the card. However, biometric samples are exposed on PoU stations (unless biometric sensor is also on card, which is believed only practical for fingerprint). Also, requires adequate on-card computer power, and additional template storage for multi-biometric use, which increases costs. Relies entirely on identity cards being invulnerable to reverse engineering (to read contents and make "lying near-clones").

Expected Architecture for NIdS

Mix of Template on Card / Match on Station and Match on Central System: Use only a subset of available templates on cards, to ensure that additional biometric checks are available on-line for higher security verification, with less risk of compromise by artefact attack and infiltrator selection (from access to lost/stolen/cloned cards).

Protect against forged/altered cards using digital signatures: Remember that this is excellent security for identity documents, beyond that currently (or recently) used for passports, etc. This is totally independent of the additional identification benefits arising from use of biometrics.

Protect communications to/from central system with end-to-end encryption: Use key partitioning to avoid widespread compromise, through reverse engineering, from improper physical access to PoU computers. Use NIR audit trail to aid detection of key compromises.

Residual Security Issues

Compromise of Central NIR System: Particularly ITSEC risks and staff subornment; leading to mass copying of data (for infiltrator selection or target selection) and for injection of false identities.

Breaking of digital signature key and creating forged cards: There is some protection from key compartmentation to contain the risk; eg change card issue key every 3 months (about 1 million cards) and force on-line checks for cards keys known to be compromised.

Successful creation of false identity by the standard application procedure: Particularly staff subornment; also use of artefacts, or other tricks, with careful enrolment supervision a good protection.

Artefact attack, more than expected or allowed for: This is a particular issue for unsupervised PoUs. One protection is to increase the number of PoU scenarios in which multi-biometric matching is required, despite extra costs and other inconveniences.

Civil Liberties Issues

Unavoidable Issue: Compulsory NIdS registration takes away the civil liberty not to register. Likewise, the requirement to attend for registration/enrolment is a reduction in civil liberties.

Not British: There is a view that the overall NIdS concept is "not British". UK citizens are not accountable to the Government for the right to be here; the Government is accountable to us, the electorate.

Big Brother: The following have been raised: watchlists, forensic use (especially fingerprints), and surveillance through the NIR audit trail. All these could be mitigated by parliament declining to approve such uses, or inserting, for example, requirements for judges' warrants.

Function Creep: which is, of course, a feature of all government.

Over-Zealous Officials: which led to ID card withdrawal after WW2.

NIR as single critical point: Is adequate protection possible?

IRN: numbering people is wrong, and politically oppressive.

Cost-Effectiveness of the Whole National Identity Scheme

Separation of costs for usage classes (types of PoU): eg border control; opening bank accounts; going to the county library. There is a good case for separating all PoU costs from costs of setting up and running the basic system: enrolment, card issue and provision of an identity service. This is because each type of PoU could (and should) have its cost-effectiveness judged on that particular specific case. Of course, the basic system needs to be justified, including on grounds of cost. This might, and probably does, require analysis of a minimum number of PoU types and consideration of their costs with those of the basic system, in order to justify implementation of the basic system. That is unless the secondary benefits (watchlists, forensic use, surveillance) together with reduction in use of multiple identities are considered adequate justification.

Approximate costs, per registered person: next slide

Approx Costs for Setting Up and Running the Basic NIdS

Item	Reg per Person
Supervision by Registration Officer: 12 reg/day; 220 days pa; £60K pa incl. overheads	**22.70**
Card Replication: 1 card every 5 years; £1.50 each	**3.00**
Enrolment Station Use: 5 year life; 2,640 reg/year; £20K cost	**1.50**
NIR System Procurement: £200 million; 47 million registrations	**3.80**
NIR Unrecoverable Running Costs: 100 staff; £60K pa incl. overheads	**1.10**
	Total £32.10

Summary of Issues Discussed

A biometric based NIdS can provide an identity certification service.

It can also provide the government with secondary benefits, through provision of templates for watchlists and forensics, and through preserving the NIR Audit Trail for retrospective surveillance. It is for parliament to decide the extent to which this is acceptable.

Biometric performance issues are largely understood; FNMR/FMR is the key measure. Performance is, or is approaching, adequate for the job; multi-biometric fusion is necessary for DMA.

Careful management of security issues is essential, including use of digital signatures and encryption; otherwise the effectiveness of the identity service would become too compromised for long-term acceptance and cost-effectiveness.

Basic NIdS costs can and should be separated from application specific costs. Costs are much better understood that benefits, which are very difficult to quantify.