UIDAI

Unique Identification Authority of India
Planning Commission,
Yojana Bhavan,
Sansad Marg,
New Delhi 110001

Biometrics Design Standards For UID Applications

Version 1.0
December 2009

Prepared by: UIDAI Committee on Biometrics

CONTENTS

1 Executive Summary

The Unique Identification Authority of India (UIDAI) was set up by the Govt. of India on 28 January 2009. The purpose of the UIDAI is to issue Unique Identification numbers to all residents in the country. The Authority set up a Biometrics Standards Committee in order to frame biometrics standards for use by the UIDAI and its partners. The first deliverable of the Committee was to frame biometric standards based on existing national and international standards, with the consensus of various government stakeholders. The second deliverable was to recommend appropriate biometrics parameters to achieve the UIDAI's mandate. The second goal of the Committee encompasses best practices, expected accuracy, interoperability, conformity and performance in biometrics standards.

After reviewing international standards and current national recommendations, the Committee concluded that the ISO 19794 series of biometrics standards for fingerprints, face and iris set by the International Standards Organization are the most suitable. These standards are widely accepted, and best embody previous experiences of the US and Europe with biometrics. The standards framed for the UIDAI are accordingly, fully compliant with the respective ISO standards, and are given in Sections 7 through 11.

The Committee notes that Face is the most commonly captured biometric, and frequently used in manual checking. However, stand-alone, automatic face recognition does not provide a high level of accuracy, and can only be used to supplement a primary biometric modality. Fingerprinting, the oldest biometric technology, has the largest market share of all biometrics modalities globally. The fingerprint industry also has a variety of suppliers and a base of experienced professionals necessary to implement the unique identity management solution at the scale that India requires. Based on these factors, the Committee recognises that a fingerprints-based biometric system shall be at the core of the UIDAI's de-duplication efforts.

The Committee however, is also conscious of the fact that de-duplication of the magnitude required by the UIDAI has never been implemented in the world. In the global context, a de-duplication accuracy of 99% has been achieved so far, using good quality fingerprints against a database of up to fifty million. Two factors however, raise uncertainty about the accuracy that can be achieved through fingerprints. First, retaining efficacy while scaling the database size from fifty million to a billion has not been adequately analyzed. Second, fingerprint quality, the most important variable for determining de-duplication accuracy, has not been studied in depth in the Indian context.

The Committee therefore held extensive meetings and discussions with international experts and technology suppliers. A technical sub-group was also formed to collect Indian fingerprints and analyze quality. Over 250,000 fingerprint images from 25,000 persons were sourced from districts of Delhi, UP, Bihar and Orissa. Nearly all the images were from rural regions, and were collected by different agencies using different capture devices, and through different operational processes. The analysis reported in Section 12.4 and the associated Annexure show that the UIDAI could obtain fingerprint quality as good as seen in developed countries, provided that proper operational procedures are followed and good quality devices are used. On the other hand there is

data to suggest that quality and therefore the accuracy drops precipitously if attention is not given to operational processes.

The demographic data (non-biometric data) is also used for improving de-duplication processes. It reduces the amount of manual labor required to establish genuine duplicates from a possible list of duplicate matches.

Further, it has also been observed that Iris, which for a long period of time was under the proprietary domain, is emerging as an important biometric modality after fingerprint and face. The accuracy and speed of iris-based systems currently deployed is promising and may be feasible in large-scale de-duplication systems.

Finally, it is possible to combine multiple biometric modalities including multiple fingerprints to increase overall de-duplication accuracy.

Recommendations

Based on the above deliberations, the Committee makes the following principal recommendations:

1. The Committee expects that the UIDAI could achieve at least 95% de-duplication accuracy using moderately good fingerprint images for a database size of 1 billion. Empirical image quality data of Indian ground conditions clearly show that such accuracy is achievable. In the global context, a de-duplication accuracy of 99% has been demonstrated to be achievable using good quality fingerprints against a database of up to fifty million.
2. In order to capture moderately good fingerprint images, a few simple but critical techniques during enrolment should be consistently followed, failing which material reduction in accuracy would occur. Manual and automated monitoring should be utilized to ensure consistent use of good enrolment practices.
3. In view of the above, the Committee feels that the UIDAI should collect photograph and ten fingerprints as per ISO standards described in Sections 8, 9 and 10.
4. Biometrics data are national assets and must be preserved in their original quality. In other words, quality must not be compromised through lossy image compression during storage or transmission.
5. While 10 finger biometric and photographs can ensure de-duplication accuracy higher than 95% depending upon quality of data collection, there may be a need to improve the accuracy and also create higher confidence level in the de-duplication process. Iris biometric technology, as explained above, is an additional emerging technology for which the Committee has defined standards. It is possible to improve de-duplication accuracy by incorporating iris. Accuracy as high as 99% for iris has been achieved using Western data. However, in the absence of empirical Indian data, it is not possible for the Committee to precisely predict the improvement in the accuracy of de-duplication due to the fusion of fingerprint and iris scores. The UIDAI can consider the use of a third biometric in iris, if they feel it is required for the Unique ID project.
6. A scheme must be designed to reward enrolling agencies for the capture of good quality images.

7. Specific best practices indicated in Section 12 should be observed in order to ensure interoperability, vendor independence, conformance to standards and improved performance.
8. The UIDAI along with other stakeholders should establish center(s) for on-going biometrics research, and provide reference implementation of enrolment process software designed for Indian conditions.

2 Introduction

The UID Authority of India (UIDAI) has been setup by the Govt. of India with a mandate to issue a unique identification number to every resident in the country. The UIDAI proposes that it create a platform to first collect the identity details of residents, and subsequently perform identity authentication services that can be used by government and commercial service providers. A key requirement of the UID system is to minimize/eliminate duplicate identities in order to improve the efficacy of the service delivery.

The UIDAI has selected the biometrics feature set as the primary method to check for duplicate identity. In order to ensure that an individual is uniquely identified in an easy and cost-effective manner, it is necessary to ensure that the captured biometric information can be used to carry out de-duplication. Consequently, for government and commercial providers to authenticate the identity at the time of service delivery, it is necessary that biometric information capture and transmission are standardized across all partners and users of the UID system.

The Government of India has in the past set up a number of expert committees to establish standards for various e-governance applications in the areas of Biometrics, Personal Identification and location codification standards. These committees have worked out standards in their respective categories, which may be uniformly applied for various e-governance standards.

As the UIDAI proposes to use biometrics for de-duplication and verification/authentication, it becomes essential to review the applicability and sufficiency of these standards in UID applications. It may also be necessary to enhance or clarify these standards,, and frame the methodology for the implementation of biometrics to ensure that they serve the specific requirements of the Authority.

3 Objective

The UIDAI biometrics committee ("the Committee") was constituted to provide the UIDAI with direction on the biometrics standards, suggest best practices and recommend biometric modalities for the UID system (Annexure I).

The objective of these biometrics specifications is to ensure consistent good quality biometric images and reliable interoperability across biometric capture devices, capture software and UID service delivery.

The success of the Unique ID is solely based on its ability to detect and eliminate duplicate identities during the enrolment process. The primary method for detecting duplicates will be through the comparison of the biometric feature set, which requires consistent, high quality images. A good biometric implementation design that ensures consistent quality from a variety of biometric capture devices is therefore, essential.

The biometrics will be captured for authentication by government departments and commercial organizations at the time of service delivery. They will invariably use capture devices and biometric software vendors different from the devices and software used by UIDAI. Consequently, biometric standards are essential to ensure reliable interoperability at reasonable cost during the authentication phase.

The purpose of this document is to identify applicable standards and recommend best practices to the UIDAI to achieve its objective.

4 Scope

- To develop biometric standards that will ensure the interoperability of devices, systems and processes used by various agencies that communicate with the UID system.
- To review the existing standards and, if required, modify/extend/enhance them so as to serve the specific requirements of the UIDAI.
- To specify design parameters of the standards that will be used for the UID system.
- To estimate the accuracy achievable using different biometric modalities in the Indian environment.
- To make recommendations to the UIDAI on the use of biometric modalities.

From the standpoint of the biometrics industry, the UID system is a civilian application of biometrics. Although the primary focus is the UID system, the Committee believes that the specifications should meet the needs of all civilian applications. The Committee considers forensic application requirements out of scope.

5 Target Audience

Any person or organization involved in designing, testing or implementing UID or UID compatible systems for the central government, state government or commercial organizations.

Any vendors and integrators of biometric devices and software targeting UID system compatibility.

6 Normative Reference

The following reference documents are indispensable for the application of this document.

IAFIS-IC-0110 (V3), WSQ Gray-scale Fingerprint Image Compression Specification 1997

ISO/IEC 15444 (all parts), Information technology – JPEG 2000 image coding system

ISO/IEC 19785-1:2006. Common biometric exchange formats framework – Part 1: Data elements specifications

ISO/IEC 19794-2:2005. Biometric data interchange formats – Part 2: Finger minutiae data

ISO/IEC 19794-4:2005. Biometric data interchange formats – Part 4: Finger Image data

ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face Image data

ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris Image data

ISO/IEC CD 19794-6.3. Biometric data interchange formats – Part 6: Iris Image data working group draft

MTR 04B0000022. (Mitre Technical Report), Margaret Lepley, Profile for 1000 Fingerprint compression, Version 1.1, April 2004. Available at http://www.mitre.org/work/tech_papers/tech_papers_04/lepley_fingerprint/lepley_fingerprint.pdf

7 Standards

In the current IT world, as interoperability between devices and IT systems becomes a growing concern, the question is not whether to use standards but which standards to use. ANSI, INCITS, CEN, Oasis and ISO are just a few of the prominent agencies with published biometrics standards. After reviewing the charter of each body and current state of biometrics in India, the Committee selected the ISO standard. Within the ISO body of biometrics standards, the Committee will use data format standards. These standards are widely supported by vendors, and are used extensively. ISO data format standards also contain the maximum empirical information on usage, interoperability and conformance.

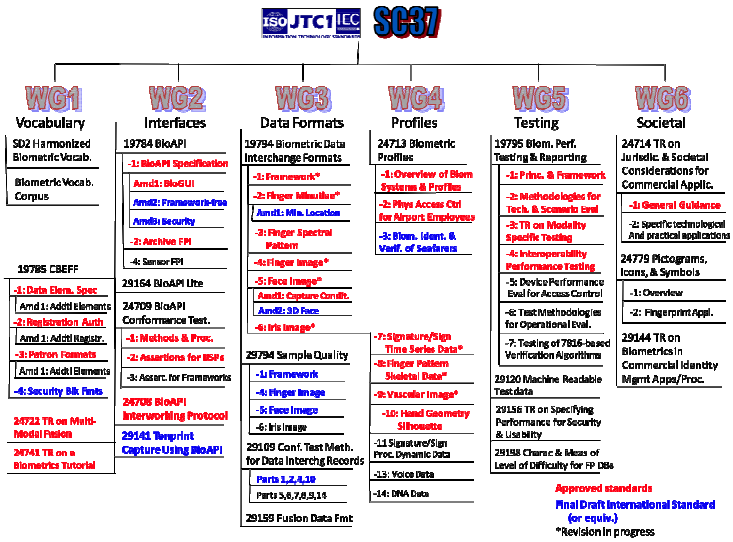

Figure 1 ISO Biometrics Standards Activity

8 Tailoring of Face Image Standards

The UIDAI Fingerprint Image Standard will adopt ISO/IEC 19794-5 Face Image Data Standard as the Indian Standard and will specify certain implementation values (tailoring) and best practices.

8.1 Section 7 Digital/Photographic requirements

The UIDAI will require face images for human visual inspection and duplicate check on a small subset. Visual inspection and automatic matching accuracy is directly related to the quality of the images. Therefore it is essential that the highest quality of images be consistently captured.

8.1.1 For Enrollment and Authentication

Defining the values for face image standards as shown in Section 7.2, table 2.

Face Image Type Code	Scan resolution (dpi)	Color Space Code	Source Type Code	Inter-eye distance (pixels)	Facial Expression Code
Full Frontal (0x01)	300	24 bit RGB (0x01)	0x02 0x06	120	0x01

8.1.2 Source Type

Static face images (Code 0x02) from a digital still-image camera are strongly recommended. Single video frames from a digital video camera (Code 0x06) are also acceptable.

16.1.3 Expression

Face images should have neutral expression (non-smiling) with both eyes open and mouth closed.

16.1.4 Pose

Roll, pitch and yaw angle should not be more than $\pm 5^0$ (Figure 4 of ISO 19794-5).

8.2 Section 7 Image Compression Algorithm

8.2.1 For Enrolment

For enrolment, uncompressed images are strongly recommended. Lossless JPEG 2000 color compression will be accepted for legacy purposes only.

16.2.2 For Authentication

Code 0x01 - JPEG 2000 compression is recommended. Maximum compression ration is 10.

8.3 Face Record Format

8.3.1 CBEFF Header

The UIDAI will not use information defined in Section 5.3 of ISO document.

8.3.2 Facial Record Header

The UIDAI will maintain single facial image.

8.3.3 Facial Information Block

The UIDAI will not use information defined in Sections 5.5.1 to 5.5.6 of ISO document.

8.3.4 Feature Point Block

The UIDAI will not use geometric feature points defined in Section 5.6 of ISO document.

9 Tailoring of Fingerprint Image Standard

The UIDAI Fingerprint Image Standard will adopt ISO/IEC 19794-4 Fingerprint Image Data Standard as Indian Standard and specify certain implementation values (tailoring) and best practices.

9.1 Section 7: Image Acquisition Requirements

The duplicate check during the enrolment phase will use 1:N matching. 1:N matching for large gallery size and high enrolment rate will require substantial computing resources. The matching time and matching accuracy is directly related to the quality of the images. Therefore it is essential that the highest quality of images be consistently captured. It is also required that all ten fingers are captured whenever physically possible.

The goal during authentication is to achieve fast overall response while permitting a wide variety of capture devices and associated software. It is sufficient to capture only one or two fingers for reliable 1:1 authentication. The image quality needs for authentication are not as stringent as in enrolment.

9.1.1 For Enrolment

Setting level 31 or higher as shown in Section 7.1, table 1

Setting level	Scan resolution (ppcm)	Scan resolution (dpi)	Pixel depth (bits)	Dynamic range (gray levels)	Certifications
31	197	500	8	200	EFTS/F

9.1.2 For Authentication

Setting level 28 or higher as shown in Section 7.1, table 2

Setting level	Scan resolution (ppcm)	Scan resolution (dpi)	Pixel depth (bits)	Dynamic range (gray levels)	Certifications
28[1]	118	300	4	12	UID
30	197	500	8	80	None

9.2 Section 8 Finger Image record Format

9.2.1 Section 8.2.14 Image compression algorithm

9.2.1.1 Enrolment

Code 0 and 1 are strongly recommended. For legacy purposes only, lossless compression of code 2, 4 and 5 will be accepted.

9.2.1.2 Authentication

Code 4, compressed – JPEG 2000 is recommended. Code 0, 1, 2 and 5 are also acceptable. Code 3 must not be used. Maximum compression ration is 15.

[1] Level 28 is not specified in FBI's Electronic Fingerprint Transmission Specifications, Appendix F (commonly referred to as EFTS/F). It has been created to accommodate certain class of new generation lower cost single finger capture devices.

9.2.2 Section 8.3.3 Finger/palm position

The valid values for finger/palm position are 0 through 10, 13 through 15.

9.2.3 Section 8.3.7 Impression type

For enrolment image, only code 0 or 9 will be used. Authentication impression can be of type 0, 1, 8 or 9.

9.2.4 Section 8.3.10 Finger/palm image data

The estimated optimal fingerprint image captured under aforementioned specification of this standard in bitmap is 7.5MB per subject.

10 Tailoring of Minutiae Format Standard

UID Minutiae Format Standard will adopt the ISO/IEC 19794-2 Minutiae Format Standard as the Indian Standard and specify certain implementation values (tailoring) and best practices.

10.1 Section 7.4.1.3 Impression Type

For enrolment image, only code[2] 0 or 9 will be used. Authentication impression can be of type 0, 1, 8 or 9.

10.2 Section 7.5 Extended Data

While the extended data area allows for the inclusion of proprietary data within the minutiae format, this is not indented to allow for alternate representation of data that can be represented in open manner, as defined in ISO/IEC 19794-2. In particular, ridge count data, core and delta data or zonal quality information shall not be represented in proprietary manner to the exclusion of publicly defined data formats.

The UID authentication process will not utilize extended data area for verification.

[2] Codes specified in ISO/IEC 19794-4, Section 8.3.7 are newer and superset of this table. Hence the reference is made to ISO/IEC 19794-4 Table 7.

11 Tailoring of Iris Standards

UID Iris Image Standard will adopt the ISO/IEC 19794-6 Iris Image Data Standard as the Indian Standard and specify certain implementation values (tailoring) and best practices. The current (2005) version is under revision. A new version (2010) is expected to clear the ISO/IEC JTC 1/SC 37 sub-committee in January 2010. Therefore all references below are to the latest (November 2009) draft of the proposed standard. The Committee will revise this section after the ISO standard is published.

11.1 Section 7.4.2.2 Kind

Allowable values are KIND-VGA (2) and KIND_CROPPED (3) in Table 5.

11.2 Section 7.4.2.4 Image data

Every effort must be made by the vendor to register Capture Device Vendor ID and Capture Device Type ID with the appropriate registration authority. It is strongly recommended that these fields as described in Table 6 not be filled with zero value.

It is strongly recommended that quality information consisting of Quality score, Quality algorithm vendor ID and Quality algorithm ID as described in Table 6, shall be provided.

12 Best Practices

Specific recommendations for each modality listed below are based on prevailing standards, best practices followed by international users and the ground reality in India.

12.1 Face

Key Decisions	Decision Type	Summary of Decisions
Enrolment		
Image capture	R	Full frontal, 24 bit color
Digital/Photographic requirements	R, S	Per ISO 19794-5 Section 7.3, 7.4, 8.3 and 8.4 with Section 8.3 of Technical Corrigendum 2. Inter-eye distance – minimum 120 pixels.
Pose	S	Per ISO 19794-5 Section 7.2.2
Expression	R, S	Neutral expression. Specified as best practices.
Illumination	S	Per ISO 19794-5 Section 7.2.7
Eye Glasses	S	Per ISO 19794-5 Section 7.2.11
Accessories	R	Permissible for medical and ethical reasons only.
Multiple samples of face	M	Yes. Recommended for automatic face recognition.
Operational	S	Per ISO 19794-5 Section 7.2.4 - 7.2.10
Assistance	R	Yes. Specified as best practices.
Segmentation and feature extraction	M	Recommended for automatic face recognition
Quality check	R	Yes. Specified as best practice.
Storage & compression	S	Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 color accepted.
Authentication		
Image capture	R	Same as enrollment
Compression	S	JPEG 2000 color compression recommended. Compression ratio to be less than 10:1.
Number of Images	R	One full frontal image

Figure 2 Face image

12.2 Fingerprint

Key Decisions	Decision Type[3]	Summary of Decisions
Enrolment		
Image capture		
Plain or rolled	R	Plain, live scan
Number of fingers	R	Ten
Device characteristics	S	Setting level 31 or above, EFTS/F certified
Quality check	R	Yes – specified as best practice
Operational		
Assistance	R	Yes – Specified as best practice
Corrective measure	R	Yes – Specified as best practice
Storage & transmission		
Compression	S	Uncompressed images strongly recommended. For legacy reasons, lossless JPEG 2000 or WSQ compression accepted.
Storage format	S	Per ISO Section 8.3. No deviation necessary
Minutiae format	S	Per ISO 19794-2. No deviation necessary.
Multi-finger fusion algorithm	R	Recommended. Application dependent.
Authentication		
Image capture		
Number of fingers	R	No minimum, no maximum. Application dependent. Recommended as best practice
Any finger option	M	Yes. Recommended as best practice
Retry	R	Maximum 5. Recommended as best practice.
Device characteristics	S	Setting level 28 or above
Transmission format	S	Per ISO. No tailoring necessary
Compression	S	JPEG 2000 compression recommended. Compression ratio to be less than 15:1
Minutiae format	S	Per ISO 19794-2. No tailoring necessary

Figure 3 Fingerprint

[3] R: Recommendation based on best practice/empirical data, S: Standard based, M: Management judgment.

12.3 Iris

Decision		Decision Type	Summary of Decision
Enrolment			
	Image	R	Two eyes, > 140 pixel image diameter (170 pixel preferred), image margin 50% left and right, 25% top and bottom of iris diameter
	Device Characteristics	R	Tethered, autofocus, continuous image capture, exposure < 33 milli-second, distance >300 mm for operator control, > 100mm enrollee control
	Operational	M	Operator controlled strongly preferred. No direct natural or artificial light reflection in the eye, indoor.
	Segmentation	R	Non-linear segmentation algorithm
	Quality Assessment	R	Per IREX II recommendations[4]
	Compression & Storage	S	ISO 19794-6 (2010) data format standard as tailored in Section 11. JPEG 2000 or PNG lossless compression, KIND_VGA of Table A.1 of ISO 19794-6 (2010).
Authentication		R, S	Same as enrollment except One or two eyes JPEG 2000 KIND_CROPPED of Table A.1

Figure 4 Iris

12.4 Biometrics Accuracy

The UIDAI's charter of assuring uniqueness across a population of 1.2 billion people mandates the biometrics goal of minimizing the False Accept Rate (FAR) within technological and economical constraints.

All published empirical data is reported using Western populations and database sizes of tens of millions. An accuracy rate (i.e., True Acceptance Rate) of 99% is reported in the test of commercial system performance[23]. Two factors however raise uncertainty on the extent of accuracy achievable through fingerprints: First, the scaling of database size from fifty million to a billion has not been adequately analyzed. Second, the fingerprint quality, the most important variable for determining accuracy, has not been studied in depth in the Indian context.

[4] IREX II study conducted by NIST will be published in April 2010. It will provide definite empirical result of impact of image quality on matching accuracy and speed. For fingerprint the analogous study resulted in creation of NFIQ, NIST Fingerprint Image Quality algorithm. We anticipate similar outcome from IREX II. IREX II will be normative annexure to ISO 19794-6 (2010).

A technical sub-group was formed to collect Indian fingerprints and analyze quality. Over 250,000 fingerprint images from 25,000 persons were sourced from districts of Delhi, UP, Bihar and Orissa. Nearly all were from rural regions, collected by different agencies using different capture devices and through different operational processes. Analysis reported in Annexure showed the UIDAI could obtain as good fingerprint quality as seen in developed countries, provided that proper operational procedures are followed and good quality devices are used. On the other hand there is data to suggest that quality and therefore the accuracy drops precipitously if attention is not given to operational processes.

Based on rather extensive empirical results compiled by NIST and a first cut of Indian data analyzed in a short period, the following broad categorization can be made

1. The UIDAI can obtain fingerprint quality as good as that seen in developed countries. There is good evidence to suggest that fingerprint data from rural India may be as good as elsewhere when proper operational procedures are followed and good quality devices are used. There is also data to suggest that quality drops precipitously if attention is not given to operational processes.
2. It is possible to closely predict the expected fingerprint recognition performance. In the experiments, at 95% confidence, the sample database of a rural region is expected to achieve similar accuracy as Western data. By extrapolating NIST analysis of Western data, it is possible to conclude that fingerprint alone is sufficient to achieve minimum accuracy level of 95%, with moderately good fingerprints images.
3. Face is an invaluable biometric for manual verification. Its potential to contribute materially to improved FAR rate is however, limited particularly because of extremely large database size and high value of target accuracy.
4. Iris can provide accuracy comparable to fingerprint. Therefore fused score of two uncorrelated modalities will provide better accuracy than any single modality and could achieve the target accuracy.

Empirical data has highlighted several non-technical factors that can impact accuracy more significantly than technical accuracy improvement efforts.

- Simple operational quality assurance. A few simple operational techniques such as keeping a wet towel or maintaining the device in good working order can be superior to squeezing an additional fraction of a percent in accuracy rates through technical improvements. An unchecked operational process can increase the false acceptance rate to over 10%.
- In the data analyzed, 2% to 5% of subjects did not have biometric records. Missing biometrics is a license to commit fraud. It is believed that the failure is due to poorly designed processes. The enrolment process when examined, had loopholes which prevented it from detecting such omissions.
- The biometric software needs to be tuned to local data. Un-tuned software can generate additional errors in the range of 2 to 3%.

13 Members

13.1 Biometrics Committee

	Name, Affiliation
1.	Dr. B. K. Gairola, DG NIC – Chairman
2.	Dr. C. Chandramauli – Registrar General of India (RGI) – Member
3.	Dr. D. S. Gangwar, Joint Secretary, Rural Development- Member
4.	Dr. A. M. Pedgaonkar, RBI – Member
5.	Mr. Pravir Vohra, ICICI – Member
6.	Prof. Deepak Phatak, IIT Bombay – Member
7.	Prof. Phalguni Gupta, IIT Kanpur – Member
8.	Mr. R. S. Sharma, DG UIDAI – Member/Convener
9.	Mr. Rajesh Mashruwala, UIDAI – Member
10.	Mr. Srikanth Nadhamuni, UIDAI – Member

13.2 Face Sub-committee

1.	Dr. Richa Singh
2.	Dr. Mayank Vatsa
3.	Mr. Rajesh Mashruwala

13.3 Fingerprint Sub-committee

1.	Prof. Phalguni Gupta
2.	Dr. A. M. Pedgaonkar
3.	Mr. Rajesh Mashruwala
4.	Dr. Mayank Vatsa

13.4 Iris Sub-committee

1.	Prof. Phalguni Gupta
2.	Dr. Mayank Vatsa
3.	Mr. Rajesh Mashruwala

Annexure I
Notification of UIDAI constituting the Committee

No.45/DG-UIDAI/2009
Government of India
Planning Commission
Unique Identification Authority of India

R No.321, Yojana Bhavan
New Delhi – 110 001

Dated : September 29, 2009

OFFICE MEMORANDUM

The UID Authority of India has been setup by the Govt. of India with a mandate to issue a unique identification number to all the residents in the country. The main objective is to improve benefits service delivery, especially to the poor and marginalised sections of the society. To deliver its mandate, the UID Authority proposes to create a platform to first collect the identity details and then to perform authentication that can be used by several govt. and private service providers. A key requirement of the UID system is to minimize/eliminate duplicate UIDs in order to improve the efficacy of the service delivery. A possible way to ensure uniqueness of IDs (so that one resident gets only one ID) is to use biometric technologies. In order to ensure that an individual is uniquely identified and authenticated in an easy and cost-effective manner, it is necessary to ensure that the biometric information which is captured is capable of carrying out the de-duplication at the time of collection of information. Further, in order to achieve interoperability it is important that the capture and use of biometric information is standardized across all the partners and users of the UID system.

The Government of India, in the past, had set up a number of expert committees for standards to be used for various e-governance applications in areas of Biometrics, Personal Identification and location Codification Standards. These committees have worked out few standards in the respective categories to be uniformly applied for various e-governance standards.

As UIDAI proposes to use biometrics for de-duplication and verification/authentication, it becomes essential to review the applicability and sufficiency of these standards in UID applications, modify/extend/enhance them to ensure that they serve the specific requirements of UIDAI and frame the methodology for its implementation.

In view of the above, a Committee for framing the Biometric Standards for UIDAI is being setup to review the existing standards and modify/extend/enhance them so as to achieve the goals and purpose of UIDAI for de-duplications and authentication.

1. Charter of the Biometric Standards Committee

- To develop biometric standards that will ensure interoperability of devices, systems and processes used by various agencies that use the UID system.
- To review the existing standards of Biometric and, if required, modify/extend/enhance them so as to serve the specific requirements of UIDAI relating to de-duplication and Authentication.

2. Composition of the Biometric Standards Committee

Following will be the composition of the Biometric Standards Committee:

1. Dr. BK Gairola, Director General, National Informatics Centre – Chairman
2. Dr. C. Chandramauli – Registrar General of India - Member
3. Dr. DS Gangwar, Jt Secretary, Min of Rural Development - Member
4. Dr. AM Padgaonkar, Reserve Bank of India – Member
5. Mr. Pravir Vora, ICICI - Member
6. Dr. Deepak Phatak, IIT Bombay - Member
7. Dr. Phalguni Gupta, IIT Kanpur – Member
8. Two Representatives from Technology Team of UIDAI – Members
9. Director General, UIDAI or his Nominee – Member/Convenor

Unique Identification Authority of India (UIDAI) will service this Committee.

The Committee will be able to invite representatives from user organisations and other Technology Experts as Special Invitees to solicit their views and advice on various aspects on the issue.

3. Technical Committee and Working Groups

The committee can also set up sub-committees that focus on various aspects of biometric standards such as fingerprints, Iris and facial image and working groups for conducting/developing reference implementations/proof-of-concept (POC) studies, specific research, field testing etc. on an as-needed basis. The Committee may meet from time to time and draft the standard document based on the feedback of sub committees and working groups and submit recommendations. The Committee may also set its own review process before recommending the final standards.

Working Groups can be created to assist the above committees by conducting proof-of-concept (POC) studies, specific research, field testing etc.

4. Review process

It is important that the standards remain unbiased, pragmatic, vendor neutral, interoperable, and cost effective. In biometrics where technology continues to progress rapidly, three parties - vendors, academia and enterprise users - have great deal of knowledge of the technology. The Committee's review process will leverage their knowledge without compromising on its charter.

The technical committee will publish a draft version of the document and solicit structured feedback from the members of the committee, technology vendors, academia and enterprise users. Such review process will also provide sufficient advance notice to the vendors to begin upgrade to their solution, thus reducing lead time between the final standards adoption and conforming solutions.

The feedback from the various groups will be reviewed by the technical committee and suitable changes made in order to incorporate useful inputs. The final draft will be sent over for a final review and then the ratified version of the standards will be released.

5. Deliverables of the committee

- Obtain consensus from Government stakeholders to adopt and use a common set of standards for interoperability, containment of biometrics system cost and wide spread propagation of Biometrics in governmental and private sectors.
- Review the existing standards of Biometric and, if required, modify/extend/enhance them so as to serve the specific requirements of UIDAI relating to de-duplication and Authentication.
- Ratify Biometrics standards from applicable base Indian and International standards, which meet needs of the UIDAI.
- Recommendation to UIDAI users to assure Interoperability of biometrics data
- Develop certification criteria for conformity, interoperability and performance.
- Maintain & Publish registry of recommended biometrics standards, interoperability recommendations and certification criteria.

6. Time-Frame

Keeping in view the commitment of UIDAI to start issuing UIDs within twelve to eighteen months, it is necessary that the Committee presents its report on standards as early as possible. Hence the Committee will present its Final Report to the undersigned on Biometric Standards to be adopted by UIDAI within 90 days of its constitution.

7. Miscellaneous

The non-official members of the Committee and Special Invitees will be reimbursed the cost of their travel and other incidental expenses as per Rules as and when they travel to attend the Committee meetings.

29.9.09

(R S Sharma)
Director General & Mission Director

Copy forwarded to the Chairman and Members of the Committee for information and necessary action.

Copy to: Cabinet Secretary/ Principal Secretary to the PM/All Secretaries to Govt. of India/All Chief Secretaries of the States/UTs for information.

Annexure II Technical Data

Biometrics Basics

Biometrics is the science of establishing the identity of an individual based on the physical, chemical or behavioural attributes of the person. The relevance of biometrics in modern society has been reinforced by the demand for large-scale identity management systems whose functionality relies on accurately determining an individual's identity. No single biometric is expected to effectively meet all the requirements imposed by all applications. In other words, no biometric is ideal, but a number of them are admissible[1].

Demographic data is used along with the biometric information to improve the de-duplication process. For example, when a duplicate is suspected, a manual review of all available information of the person will also include a review of the demographic data.

Face

Photos of the face are commonly used in various types of identification cards and there is wide public acceptance for this biometric identifier. Face recognition systems are the least intrusive type of biometric sampling system, requiring no contact or even awareness of the subject. The face biometric can work with legacy photographs, videotapes and other image sources.

A face needs to be well lighted using controlled light sources for automated face authentication systems to work well. There are many other such technical challenges associated with robust face recognition. Face is currently a poor biometric for use in de-duplication. It performs better in verification but not at the accuracy rates that are sometimes claimed. An obvious way for an undesirable person to avoid face identification is by the use of disguise, which will cause False Negatives in a screening application. In general, it is a good biometric identifier for small-scale verification applications.

Fingerprint

There is a long tradition in the use of fingerprints for identification. Fingerprints are easily sampled with low-cost fingerprint scanners. They can also be sampled by traditional low-tech means and then cheaply and easily converted into digital images. Fingerprints also lend themselves very well to forensic investigation.

There is a large variation in the quality of fingerprints within the population. The appearance of a person's fingerprint depends on age, dirt, and cuts and worn fingers, i.e., on the occupation and lifestyle of the person in general. Sampling of the fingerprint is through contact, i.e., pressing the finger against the platen of a fingerprint reader. As a result, there can be technical problems because of the contact nature of acquisition and problems related to the cleanliness of the finger and the platen. Additionally, there are people who may not have one or more fingers [5].

Fingerprint technology constitutes approximately half of the total biometrics market[5].

Iris

The iris is the annular region of the eye, bounded by the pupil and sclera on either side. Iris is widely believed to be the most accurate biometric, especially when it comes to False Accept Rates. Therefore, the iris would be a good biometric for pure de-

[5] IDC & Acuity Market Research Reports.

duplication applications. The iris sample acquisition is done without physical contact and without too much inconvenience to the person whose iris image is being acquired. Iris has no association with law enforcement and has not received negative press and may therefore be more readily accepted.

There are few legacy databases and not much legacy infrastructure for collection of the iris biometric. Large-scale deployment is consequently impeded by the lack of an installed base. This will make the upfront investment much higher. Since the iris is small, sampling the iris pattern requires a lot of user cooperation or the use of complex and expensive devices. The performance of iris authentication can be impaired by the use of spectacles or contact lenses. Also, some people may be missing one or both eyes while others may not have the motor control necessary to reliably enroll in an iris based system.

Until recently, iris code representation and matching was proprietary and patented. Iris is emerging as the third standard biometric identifier after expiration of patents and changes in vendor practices.

The gross false accept and false reject error rates associated with the fingerprint, face and iris modalities reported in literature are shown in Figure 5 [2].

Biometric identifier	**Reference**	**FRR**	**FAR**
Fingerprint	NIST FpVTE	0.1%	1%
Face	NIST FRVT	10%	1%
Voice	NIST 2004	5-10%	2-5%
Iris	ITIRT	0.99%	0.94%

Figure 5 FAR and FRR error rates

Face Image Best Practices

Summary

Face images will be used primarily for human visual inspection. However, automatic face recognition may be used as the secondary means of authentication/de-duplication. Figure 6 summarizes key decisions for face images.

Key Decisions	Decision Type	Summary of Decisions
Enrolment		
Image capture	R	Full frontal, 24 bit color Inter-eye distance – minimum 120 pixels.
Digital/Photographic requirements	R, S	Per ISO 19794-5 Section 7.3, 7.4, 8.3 and 8.4 with Section 8.3 of Technical Corrigendum 2.
Pose	S	Per ISO 19794-5 Section 7.2.2
Expression	R, S	Neutral expression. Specified as best practices.
Illumination	S	Per ISO 19794-5 Section 7.2.7
Eye Glasses	S	Per ISO 19794-5 Section 7.2.11
Accessories	R	Permissible for medical and ethical reasons only.
Multiple samples of face	M	Yes. Recommended for automatic face recognition.
Operational	S	Per ISO 19794-5 Section 7.2.4 - 7.2.10
Assistance	R	Yes. Specified as best practices.
Segmentation and feature extraction	M	Recommended for automatic face recognition
Quality check	R	Yes. Specified as best practice.
Storage & compression	S	Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 color accepted.
Authentication		
Image capture	R	Same as enrollment
Compression	S	JPEG 2000 color compression recommended. Compression ratio to be less than 10:1.
Number of Images	R	One full frontal image

Figure 6 Face

Enrolment

Face image capture

Full frontal face image provides sufficient information for both human visual inspection (by operator) and automatic face recognition algorithms. In order to obtain a good quality image, 24-bit color image with minimum 90 pixels of inter-eye distance is required. The Committee recommends at least 120 pixels for optimum quality. The image should contain well-focused nose to ear and chin to crown region. In special circumstances, assistance may also be provided but in no case should the face or body part (hand, arms) of the assisting person or any object appear in the photograph.

Digital/Photographic requirements

In the typical enrolment setup, a computer will be connected to the biometrics devices to constitute the enrolment station. A tethered biometrics device provides several advantages over a stand-alone device. First, it allows the images to be associated with enrollee demographic data at the point of capture, thus reducing possible errors. In villages where power source may be difficult to obtain, it is simpler to supply power from the computer.

For capturing face image, it is simpler for the operator to adjust the camera instead of the enrollee to position himself/herself at the right distance or in the right posture. The capture device should use auto focus and auto-capture functions. The output image should not suffer from motion blur, over or under exposure, unnatural colored lighting, and radial distortion. Interlaced video frames are not allowed.

Pose

Face image should be full frontal with 0^0 of yaw, pitch and roll angles. However, in operational conditions, variation of $\pm 5^0$ is permissible.

Expression

Expression strongly affects the performance of automatic face recognition and also affects accurate visual inspection by humans. It is strongly recommended that the face should be captured with neutral (non-smiling) expression, teeth closed and both eyes open.

Illumination

Poor illumination has high impact on the performance of face recognition. It is difficult for human operators as well to analyze and recognize face images with poor illumination. Proper and equally distributed lighting mechanism should be used such that there are no shadows over the face, no shadows in eye sockets, and no hot spots.

Eye Glasses

Face images with and without eyeglasses may have an impact on face recognition. The impact is greater if the glasses automatically tint under illumination. If the person normally wears glasses, it is recommended that the photograph be taken with glasses. However, the glasses should be clear and transparent so that pupils and iris are visible. If the glasses are with tint, then direct and background lighting sources should be tuned accordingly.

Accessories

Use of accessories that cover any region of the face is strongly discouraged. However, accessories like eye patches are allowed due to medical reasons. Further, accessories like turban are also allowed due to ethical reasons.

Multiple samples of face

For visual inspection by humans, the single face image of a person is sufficient. However, for de-duplication and authentication of individuals who do not have fingerprints, automatic face recognition is recommended. To perform accurate authentication in such cases, capture of multiple face images is strongly recommended during enrolment. There should be three samples, out of which one should be frontal image with yaw, pitch and roll angle as 0^0. The other two images should be left and right semi profile with yaw as $\pm 20^0$ to $\pm 30^0$, and the roll and pitch should be 0^0.

Operational
Similar to fingerprints, the single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, operator training and assistance are important for yielding good quality images. Operators will be trained to obtain the best possible face images that satisfy requirements.

Segmentation and feature extraction
Segmentation and feature extraction are only required for automatic face recognition algorithms. The algorithms for both remain proprietary.

Quality check
Image quality is one of the most important factors for both human inspection and automatic face recognition algorithms. The quality assessment algorithm should encode parameters like illumination, pose, blur, noise, resolution, inter-eye distance, image height and width, and horizontal and vertical position of the face. The quality assessment algorithm should be used at the time of enrolment to determine the quality score of the captured face image and image is stored only if it meets a certain quality threshold.

Storage and Compression
According to Figures 12 and 13 of ISO face image standards, the performance of face recognition algorithms reduce significantly if the compression factor is greater than 10. Further, as mentioned previously, these are our national assets and should be captured and stored for long-term use. For preserving the quality of image, it is strongly recommended that uncompressed images should be stored in the database.

Authentication
The authentication process consists of steps similar to enrolment.

Image Capture
Image capture for 1:1 verification should also follow standards for enrolment as defined earlier in this Section.

Compression
For verification, images with JPEG 2000 compression ration of 10 will suffice. As per ISO standards, the image size after compression should not be less than 11 KB.

Number of Images
For both manual and automatic authentication, a single full frontal face image is sufficient. The captured image should conform to the digital/photographic requirements and quality thresholds mentioned above in the enrolment section.

Fingerprint Best Practices

Summary

Figure 7 summarizes the key parameters for fingerprint. The Committee further classifies the decision into

1. Standards based (S): Do ISO or other standard bodies directly provide available choices?
2. Recommendation based (R): Are there studies that provide sufficient evidence for us to make an informed decision?
3. Management judgment (M): Management decision based on project context.

The remaining section has a brief explanation of each decision.

Key Decisions	Decision Type	Summary of Decisions
Enrolment		
Image capture		
Plain or rolled	R	Plain, live scan
Number of fingers	R	Ten
Device characteristics	S	Setting level 31 or above, EFTS/F certified
Quality check	R	Yes – specified as best practice. Avoid NFIQ quality 4 and 5 level fingerprints.
Operational		
Assistance	R	Yes – Specified as best practice
Corrective measure	R	Yes – Specified as best practice
Storage & transmission		
Compression	S	Uncompressed image strongly recommended. For legacy reasons, lossless JPEG 2000 or WSQ compression accepted.
Storage format	S	Per ISO Section 8.3. No deviation necessary
Minutiae format	S	Per ISO 19794-2. No deviation necessary.
Multi-finger fusion algorithm	R	Recommended. Application dependent.
Authentication		
Image capture		
Number of fingers	R	No minimum, no maximum. Application dependent. Recommended as best practice
Any finger option	M	Yes. Recommended as best practice
Retry	R	Maximum 5. Recommended as best practice.
Device characteristics	S	Setting level 28 or above
Transmission format	S	Per ISO. No tailoring necessary
Compression	S	JPEG 2000 compression recommended. Compression ratio to be less than 15:1
Minutiae format	S	Per ISO 19794-2. No tailoring necessary

Figure 7 Fingerprint

Enrolment

The enrolment process can be broken down into image capture ("client") and de-duplication ("server") side components. The client side captures the image, performs local processing and storage. The server side receives the image, performs quality check and finally executes the computational intensive task of duplicate checking against the gallery.

Image capture

During image capture, the factors to consider are:

1. Type of image and number of fingers to capture
2. Device used for capturing the image
3. Immediate processing including segmentation of slap, sequencing of fingers, rotational correction and quality check of image
4. Storage when the images need to be stored

Plain or rolled

The rolled image, common in forensic applications, contains twice as much information as the plain image. The plain image is easier to capture. A slap capture device can capture up to four plain fingers in one scan. The rolled image in contrast, must be captured one finger at a time. Rolled images requires operator guiding the rolling of each finger. The operation difficulty in capturing rolled image rules out its use in the UID system.

Number of fingers

In general, every additional finger increases accuracy and improves matching speed. Quality of finger image among the fingers is correlated. Still, two poor quality finger images are better than one poor quality finger image. Considering the fingerprint quality of rural workers, the Committee recommends capturing prints of all ten fingers, the maximum possible.

Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. A higher resolution device does not necessarily produce better images[6]. The biometrics sample captured during enrolment needs to be the best sample possible. Therefore following best practices of leading countries, the Committee recommends the use of EFTS/F certified devices that operate at level 31 or above.

Capture & quality check

Once the image has been captured, one can perform basic quality check and image improvement. The enrollee must be asked to retry enrolling if the image quality is poor. The algorithm can assign image quality score. The quality threshold score is an important decision. Images captured with a NIST Fingerprint Image Quality (NFIQ) value of 4 or 5 normally should not be used for enrolment purposes.

---

[6] It should be noted that two devices with identical scan resolution, pixel depth and dynamic range do not provide similar quality images. A number of laboratory tests have shown that a 500 dpi device from one vendor performs better than a 1000 dpi device of another vendor. Nevertheless, these attributes are the only transparent way to specify the minimum device requirements.

Operational

The single most important factor in obtaining better image quality is the operational process. While there are many qualitative factors in designing good operational processes, the following have been shown to be critical factors:

1. Operator Assistance: Operators will be trained to guide the enrollee's hand and apply pressure if necessary to obtain best possible image quality.
2. Corrective measures & retries: If the initial capture is unsatisfactory, the operator will be trained to provide corrective measures such as wiping fingers with a wet cloth or applying lotion. Only after all such measures are exhausted in five attempts, will the operator be able to override the (forced capture) quality gate.

Storage and Transmission

Once the quality check is complete, the image needs to be retained. The data format of storage should be such that other applications can access the data.

Compression

Biometric data are national assets and should be captured and stored for long-term use. To preserve the quality, the Committee strongly recommends uncompressed images. Transmission of images may be made in JPEG 2000 or WSQ lossless compression for legacy or compatibility purposes. Any form of lossy compression is not accepted. In uncompressed mode, the total storage required for the entire population is 10,000 TB.

Storage format

ISO standard prescribed format is sufficient for our needs.

De-duplication minutiae format

The minutiae representation has been standardized. However, the standardization allows vendor proprietary data fields. The trade-off is between performance and accuracy through enhanced minutiae data versus higher level of vendor dependence. Based on the accuracy and performance trade-offs reported by NIST, it is acceptable to use the proprietary format of the extractor-matcher of the vendor selected for de-duplication.

Multi-finger fusion

Different algorithms are available to obtain consolidated score [7] and [28]. The selection of the algorithm will make material difference to the overall accuracy. ISO and other bodies do not make recommendations, nor do they provide empirical study. The UIDAI will conduct its own analysis to identify the best multi-finger fusion algorithm.

Authentication

The authentication process consists of steps similar to the enrolment process, but its requirements for accuracy, performance and interoperability are different. Since the authentication process is performing 1:1 verification, the captured image may be of lower quality compared to the image captured during the enrolment process.

Image capture

Number of fingers

It is obvious that a fewer number of fingers should be required for verification to achieve a satisfactory accuracy target. A single finger will be sufficient to provide the minimum standard of accuracy requirements. Applications requiring higher levels of accuracy may need additional fingers.

Any finger option

The normal practice is to use one specific finger, say the index finger for verification. However, current technology could allow the person to scan any finger. This is not merely a question of convenience. Certain fingers, depending on the condition of the finger, will perform better in matching. While one cannot easily determine this a priori, any frequent user will learn it by experience. This improves subsequent user experience and could potentially improve match accuracy.

Retry

The decision on number of retries has different implications during authentication. In case of enrolment, the final decision is to take the "best possible" image. The operator can thus "force capture". In case of authentication, the operator needs to find an alternate method of authentication if fingerprint verification fails. The operator/application would not know the cause of verification failure. The failure could be because the fingerprint did not match or image capture did not produce sufficient quality image for matching. In both cases, the match score is low enough for the system to declare "no match". A timeout will be implemented in service after five attempts.

Device characteristics

Device characteristics cover scan resolution, pixel depth and dynamic range. Higher resolution does not necessarily produce better images. Considering the UIDAI's goal of making authentication ubiquitous and the availability of low cost new technology devices, the Committee has defined a new standard for the scanner used in the authentication process. It is envisioned that the UIDAI will provide certification criteria for this standard.

Transmission format

The captured image needs to be sent to the UID server for matching in real time. Two factors will decide the format of the image to be sent. If the transmission bandwidth is low, it is prudent to send as little data as possible. On the other hand if the computing device associated with the capture device has very limited processing power, it is prudent to do minimal amount of local computation. In the first case, the transmission will contain extracted minutiae. In the second, it will contain the compressed raw image. For example, a capture device connected to a computer communicating over a mobile network could send minutiae by performing local extraction. A dedicated image capture device with built-in network connectivity is able to do little local processing and may send raw image.

The UID software will support raw image format, compressed image format as well as ISO standard minutiae format to be transmitted, in order to provide maximum flexibility during authentication. It is understood that raw or compressed image will give a higher level of accuracy.

Compression

If the raw image is to be sent, JPEG 2000 compression is recommended, WSQ compression may be acceptable for legacy purposes. A compression of up to 15 is acceptable. While uncompressed image will be accepted, it is not recommended. JPEG compression is not accepted. There is sufficient data to indicate that compression ratio of 15 does not affect verification accuracy. Compression is not relevant if minutiae data is to be sent for verification.

Minutiae format

As discussed in the previous section, the biometric sample being transmitted could be minutiae data or image. If the data is minutiae and the UID server has matcher that best pairs with the extractor used by the authenticating agency, it will use the proprietary data. If the server does not have matching matcher, it will only use “standard” minutiae data.

Iris Image Best Practices

Summary

Compared to fingerprinting, iris capture is less studied and less standardized. For example, fingerprint scanners are tested and certified per EFTS/F standard. No such equivalent iris device certification is available. It is necessary to provide greater number of parameter specifications to ensure quality iris capture.

Figure 8 summarizes key decisions for UIDAI iris design.

Decision		Decision Type	Summary of Decision
Enrolment			
	Image	R	Two eyes, > 140 pixel image diameter (170 pixel preferred), image margin 50% left and right, 25% top and bottom of iris diameter
	Device Characteristics	R	Tethered, autofocus, continuous image capture, exposure < 33 milli-second, distance >300 mm for operator control, > 100mm enrollee control
	Operational	M, R	Operator controlled strongly preferred. No direct natural or artificial light reflection in the eye, capture location: indoor.
	Quality Assessment	R	Per IREX II recommendations[7]
	Compression & Storage	S	ISO 19794-6 (2010) data format standard as tailored in Section 11. JPEG 2000 or PNG lossless compression, KIND_VGA of Table A.1 of ISO 19794-6 (2010).
Authentication		R, S	Same as enrollment except One and/or two eyes JPEG 2000 KIND_CROPPED of Table A.1

Figure 8 Iris

The remaining section has a brief explanation of each decision.

[7] IREX II study conducted by NIST will be published in April 2010. It will provide definite empirical result of impact of image quality on matching accuracy and speed. For fingerprint the analogous study resulted in creation of NFIQ, NIST Fingerprint Image Quality algorithm. IREX II will be a normative annexure to ISO 19794-6 (2010).

Enrolment

Iris image

Capture of two eyes simultaneously provides several advantages[8]. Iris pattern of each eye is not correlated, giving two independent biometric feature sets. It assures correct assignment of left and right eyes and allows for more accurate estimation of roll angle.

In order to obtain good quality template, the iris image diameter should be minimum 140 native pixels. The Committee recommends 170 pixels for optimum quality.

In order to retain sufficient image surrounding of the iris for the purpose of identifying the left or right eye as well as for a more accurate iris segmentation, the margins around the iris portion of the image need to be at least 50% of the iris diameter on the left and right sides of the image, and a least 25% of the iris diameter on the top and bottom of the image.

Device Characteristics

In the typical enrolment setup, a computer will be connected to the biometrics devices to constitute the enrolment station. A tethered biometrics device provides several advantages over a stand-alone device. First, it allows the images to be associated with the enrollee demographic data at the point of capture, thus reducing possible errors. In villages where a power source may be difficult to obtain, it is simpler to supply power from the computer.

Iris capture is a new experience for the public[34]. It is faster and simpler for the operator to adjust the camera instead of the enrollee positioning himself/herself at the right distance or in the right posture. It is recommended that the capture device should be more than 300 mm away from the enrollee to be considered non-intrusive. The capture device should use auto focus and auto-capture functions. In special circumstances where the enrollee has to position himself or herself, the capture device should be more than 100mm away but the device should use a visor or other mechanical alignment aid to enable the enrollee to position themselves.

In order to provide an acceptable level of usability and ease of alignment, the camera must allow for some variability in the position of the iris center relative to the camera. This variability is defined by position tolerances in the horizontal, vertical, and axial dimensions that together define a volume (the “capture volume”) within which the center of the iris must be located in order to enable image capture. For two eye capture devices, the capture volume dimensions for devices without mechanical alignment aids are 19 mm wide, 14 mm high, and 20 mm deep, and for devices with such aids, 19 mm wide, 14 mm high, and 12 mm deep.

The ability of an iris image capture device to suppress motion blur and to freeze motion, is a function of exposure time. The maximum allowable value for the exposure time is less than 33 ms, recommended being 15ms.

The iris image capture device must be capable of capturing light in the range of 700 to 900 nanometers. The camera’s near infrared illuminator(s) must have a controlled spectral content, such that the overall spectral imaging sensitivity, including the sensor characteristics, transfers at least 35% of the power per any 100 nm-wide sub-band of the 700 to 900 nm range.

[8] Material derived from [32]

The iris image capture sensor shall use progressive scanning.

In order to achieve acceptable time-to-capture and FTA rates, the iris image sampling frequency must be at least 5 frames per second.

The capture devices typically provide infrared lighting using LEDs to illuminate the iris. The illumination is in a range partly visible to the human eye. Illumination shall be compliant with illumination standard IEC 825-1 and safety specification ISO 60825-1.

In order to achieve acceptable recognition accuracy, the iris acquisition sensor must achieve a signal-to-noise ration of at least 36dB.

Within the frequency range of interest, 700 to 900 nm, the iris sensor shall generate images with at least 8 bits per pixel.

Operational considerations

As mentioned earlier, it is strongly recommended that the operator and not the enrollee handle the capture device. The enrollee will be required to sit (or stand) in a fixed position, like taking a portrait photograph; the operator will adjust the camera.

The iris capture device or the connected computer shall be able to measure the iris image quality. The best practice recommendation is that an initial image quality assessment should be done to provide feedback to the operator during the capture process. The device should alert the operator if the captured iris image is of insufficient quality.

The iris capture process is sensitive to ambient light. No direct or artificial light should directly reflect off enrollee's eyes.

Segmentation and feature extraction

Segmentation and feature extraction remain proprietary. As reported in the IREX study, the vendor providing segmentation does not have to be the vendor providing matching algorithm. In fact, best of breed selection appear to be superior to any single-vendor solution.

Quality assessment

It has been noted that image quality is the single most important factor for match accuracy. IREX II study is underway to quantify and provide best practices recommendations on the image quality. The report, expected in April 2010, will become the normative annexure to ISO 19794-6 (2010). Therefore the Committee will defer detailed quality recommendations until publication of the standard.
One method widely used for ensuring good iris images is recommended here. An Iris camera takes streaming images. It is recommended that the device take successive 3 to 7 images and use local matching algorithm to match them against each other (after feature extraction). The image is considered to be of satisfactory quality if hamming distance of the match is below 0.1.

Compression and storage

The iris images, like fingerprints are considered to be national assets. They should be stored in ISO standard format using either JPEG 2000 or PNG lossless compression (KIND_VGA). It is expected that each enrollee will require 150 Kbytes of storage space, thus requiring total storage space of 200 Terabytes for the entire population.

Authentication

For 1:1 verification, any one eye will suffice, though application may require higher-level assurance whereby both eyes can be verified. Iris verification requires the image to be sent to the server for matching. It is recommended that the image be compressed to KIND_CROPPED_AND_MASKED or KIND_CROPPED using JPEG 2000. Resulting image size will between 2KB to 10 KB. Any of the larger formats specified by the ISO standard are acceptable, though not necessary.

Biometrics Accuracy

The consequences of FAR and FRR during authentication are central to the judicial design of the UID system. FAR determines potential number of duplicates, FRR determines number of enrolments necessitating manual check, hence labor cost. While trade-off between the two rates is certainly possible, there are upper bound requirements for each. Upper bound for each rate is set at 1%.

No empirical study is available to estimate the accuracy achievable for fingerprint under Indian conditions. Indian conditions are unique in two ways:

- Larger percentage of population is employed in manual labor, which normally produces poorer biometric samples.
- Biometric capture process in rural and mobile environment is less controllable compared to the environmental conditions in which Western data is collected.

To estimate achievable accuracy under Indian conditions, following methodology was employed:

1. Estimate achievable accuracy under Western conditions for a one billion sized database.
2. Estimate difference in image quality between Western and Indian conditions.
3. Using image quality, estimate change in achievable accuracy under Indian conditions.

There is no indication to believe that iris accuracy changes from one racial/geographical population to another. However, no definitive study is available.

Step 1: Estimating achievable accuracy

NIST reports FAR of 0.07% at FRR 4.4% for 6 million fingerprint gallery size using two plain fingers [21]. Similar results were reported for FBI's IAFIS System of 46M samples. It is safe to conclude that 99% accuracy (TAR) can be achieved for database size of 50 million.

	Thresholds 1300, 1880		Thresholds 1400, 2025		
Shape Filter	FAR	TAR	FAR	TAR	Matches per Second
Off	0.30%	96.3%	0.07%	95.6%	734K
On	0.32%	96.1%	0.07%	95.5%	1035K

Figure 9 Two-finger identification accuracy

Several NIST reports allow us to estimate the scaling of above data for larger gallery size and for ten fingers.

- False Acceptance Rate is linearly proportional to gallery size at constant TAR as shown in Figure 11.
- False Rejection Rate does not vary over gallery size as shown in Figure 12.
- Based on these findings, one can expect that on a database size that is 200 times larger (1.2 billion versus 6 million), the same system will have an FAR of

approximately 0.07*200 = 14%. The FRR can be expected to be about 4% based on matching of 2 finger plain fingerprints.

- Figure 10 lists effect on FAR by increasing the number of fingers for the same FRR [22].

Number of Fingers	FRR %	FAR %
2	10.3	29.2
10	10.9	0.0

Figure 10 Accuracy of multiple fingers

- Based on the above and reviewing underlying data, one can ballpark a 1,000 improvement in FAR between two-finger matching and ten-finger matching (all other things being equal). So the estimated FAR estimate of 14% should be expected to be 1,000 times less, that is, to 0.14% at FRR rate of 4%. Using further conversation factor of 10X change in FAR results in 2X change in FRR, this number is the equivalent of *FAR 1.4% at FRR rate of 2%.* In other words, NIST data indicates de-duplication accuracy (TAR) greater than 95% is achievable for ten-finger matching against a database size of one billion.

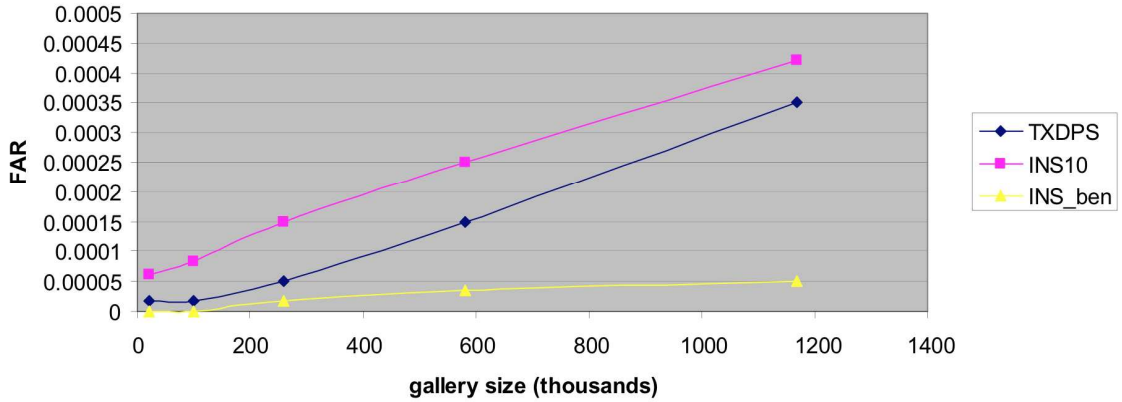

Figure 11 FAR as function of gallery size

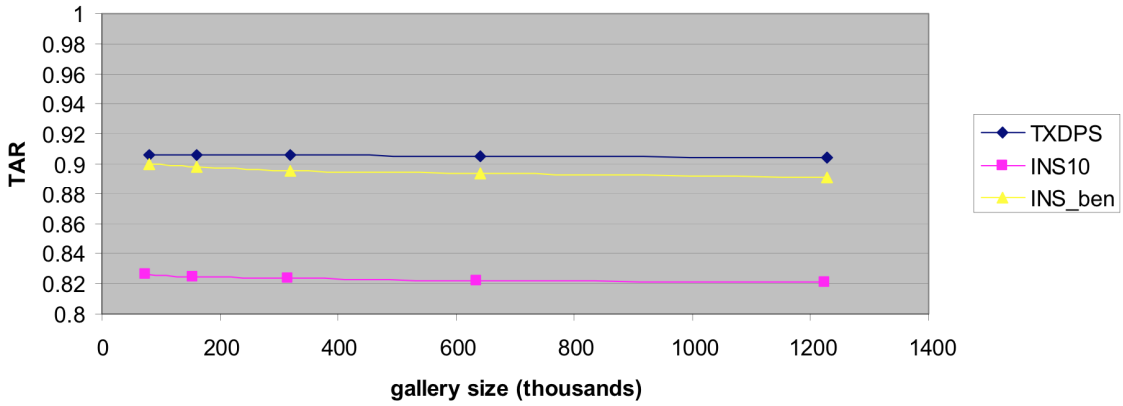

Figure 12 TAR as function of gallery size

Step 2: Image quality difference

It has been shown that match rates accuracy can be estimated from the fingerprint image quality score. NIST classifies scores into five bins. Western data accuracy rates for the bins are shown in Figure 13. Bins 1 and 2 are nearly identical, producing close to 99% true match in 1:1 verification. Bins 4 and 5 result in unacceptably low true match rates. Of particular note is bin 5, which could result in as low as 80% match rate (or 20% false accept rate).

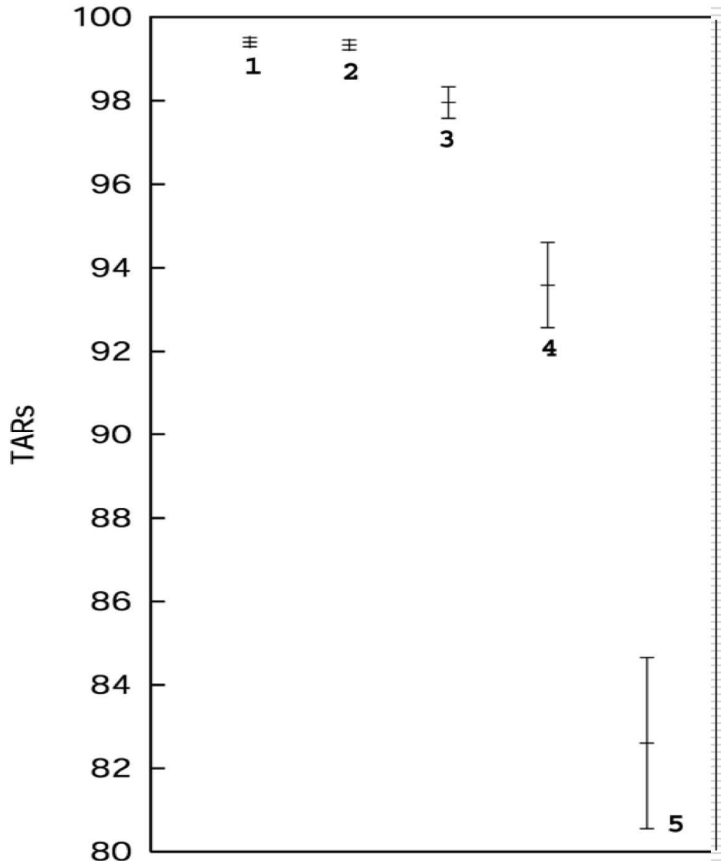

Figure 13 Accuracy Range by image quality

In a "typical" sample analyzed to arrive at the above rate[24], NIST has bin distribution shown in Figure 14 and Figure 15. Bins 4 and 5 in both datasets are less than 5% of the total sample.

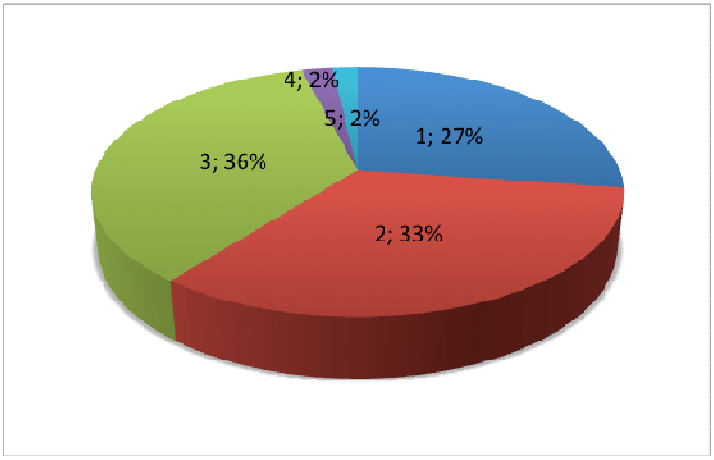

Figure 14 US-VISIT image quality distribution for right index finger

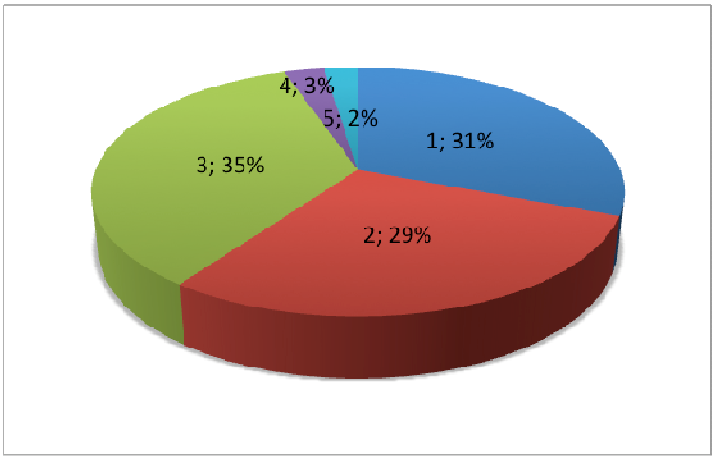

Figure 15 US-VISIT image quality distribution for left index finger

Indian Ground Conditions

The research team at IIIT Delhi focused on the ability to leverage image quality assessment tools in (1) analyzing the input biometric samples that are obtained from diverse, disparate sensors and (2) characterizing the samples based on the quality and amount of information present. Using three fingerprint databases, fingerprint image quality based experimental evaluation was performed.

1. DB1. This database contains images from 27 urban individuals (or 1350 images) and 81 rural individuals (or 1620 images). This database is prepared using single impression sensor meeting FIPS 201 APL and FBI Image Quality Specifications.
2. DB2. Images captured using slap scanner. This database contains slap images from over 20,000 individuals. Each slap fingerprint image was segmented using a commercial segmentation tool. After segmentation, the database contained 200K images. The four-finger slap sensor was EFTS/F certified and operated at level 31.
3. DB3. Pre-segmented rural slap database pertaining to about 5600 individuals (around 56,000 images). The four-finger slap sensor was EFTS/F certified and operated at level 31.

Using DB1, experimental test bed and statistical tests were prepared, followed by evaluation using DB2 and DB3. Using NIST provided Fingerprint Image Quality software (NFIQ), images were classified in to bins according to the image quality score. The bin

distributions for Indian databases are shown in Figure 16 through Figure 19. Of particular interest is significantly large bin 4 & 5 numbers for DB2 as well as DB1 rural sample. In contract, DB3, another rural area shows exceptionally high bins 1 and 2.

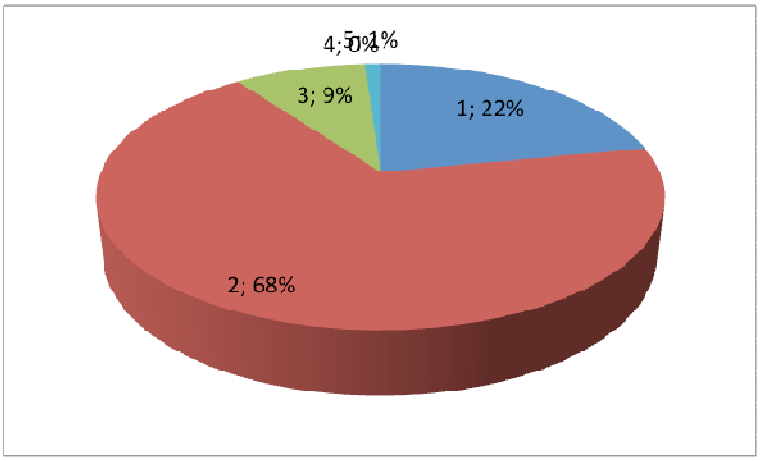

Figure 16 Image quality score distribution for DB1 Urban sample

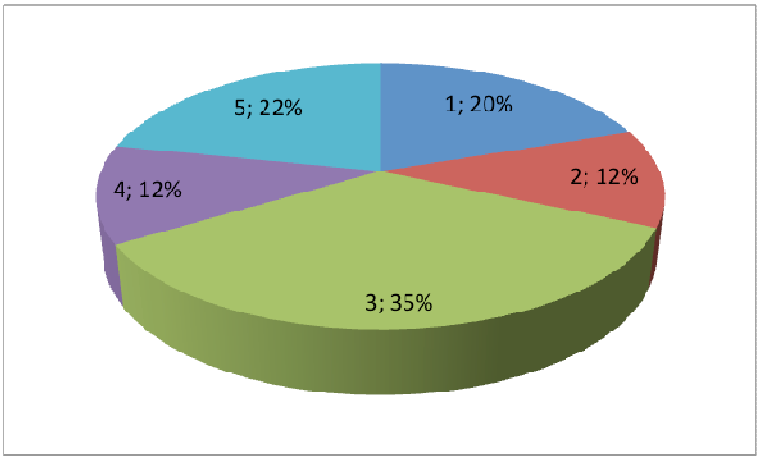

Figure 17 Image quality score distribution for DB1 Rural sample

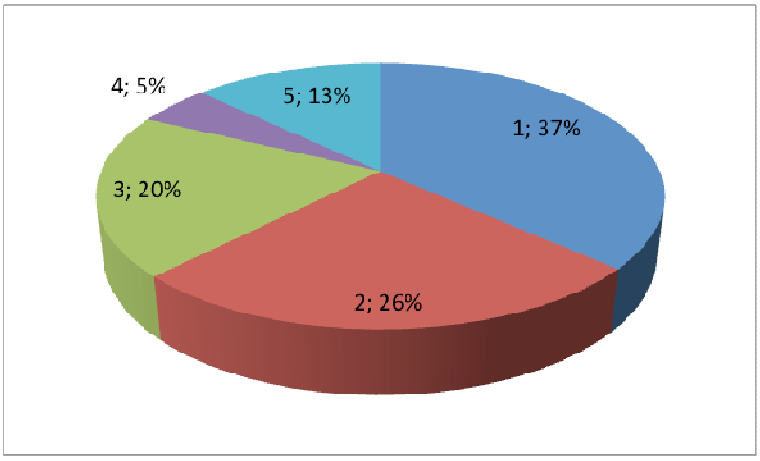

Figure 18 Image quality distribution for DB2

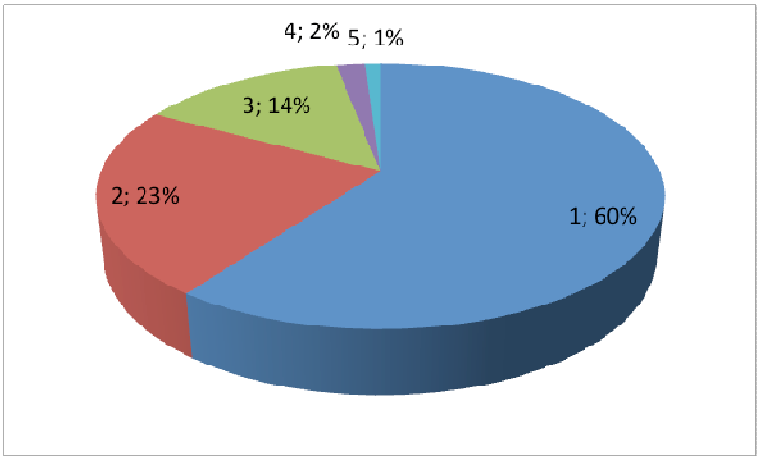

Figure 19 Image quality distribution for DB3

Step 3 Comparison & quality estimates

Since, DB2 and DB3 databases have only a single impression per finger, it is impossible to compute ROC or CMC plots and compute recognition accuracies. However, using existing Western results[24], it is possible to closely predict the expected fingerprint recognition performance.

Figure 20 and Figure 22 compare quality of left and right index finger respectively. Against x axis of accuracy (FAR), it shows cumulative bin score. Line over the Western curve (blue line) indicates that expected accuracy of the sample will be better than that of the Western population. Any points below the Western curve indicate that expected accuracy of that sample will be worse than the Western population.

DB3 shows quality superior to Western image quality while DB2 shows significantly inferior quality. While both samples are from two different rural areas of two different states, the expected accuracy is vastly different.

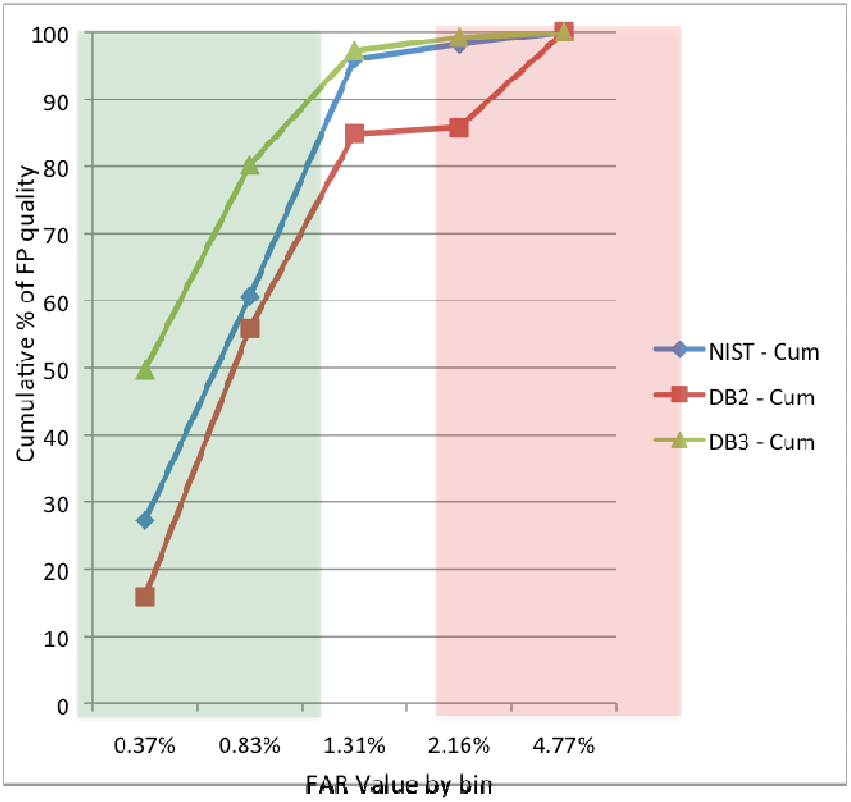

Figure 20 Right index finger comparison

Source	Bin 1	Bin 2	Bin 3	Bin 4	Bin 5
	0.37%	0.83%	1.31%	2.16%	4.77%
NIST	27.28	33.32	35.37	2.23	1.8
NIST - Cum	27.28	60.6	95.97	98.2	100
DB2	15.87	40.08	28.88	0.99	14.18
DB2 - Cum	15.87	55.95	84.83	85.82	100.00
DB3	49.73	30.51	16.97	2	0.79
DB3 - Cum	49.73	80.24	97.21	99.21	100.00

Figure 21 Right index finger numerical data

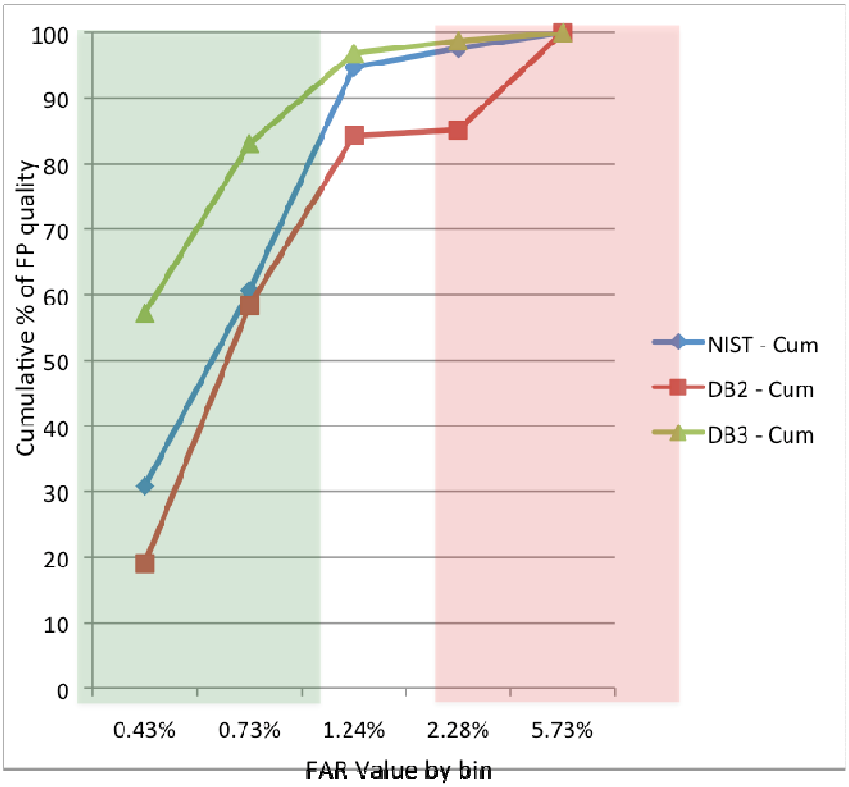

Figure 22 Left index finger comparison

Source	Bin 1	Bin 2	Bin 3	Bin 4	Bin 5
	0.43%	0.73%	1.24%	2.28%	5.73%
NIST	30.83	29.78	34.08	2.88	2.43
NIST - Cum	30.83	60.61	94.69	97.57	100
DB2	18.99	39.36	25.87	0.90	14.88
DB2 - Cum	18.99	58.35	84.22	85.12	100.00
DB3	57.25	25.77	13.8	1.87	1.31
DB3 - Cum	57.25	83.02	96.82	98.69	100.00

Figure 23 Left index finger comparison

Conclusions

NFIQ results on the databases seem to be encouraging especially if the fingerprint images are captured using good operational processes. For the majority of images, quality scores vary from excellent to good. Using these images, the typical performance of fingerprint feature extraction and matching should meet expectations. Therefore, to achieve good recognition accuracy, good quality images should be collected using optimized operational mechanisms and good sensors.

- The UIDAI can achieve fingerprint accuracy of a quality similar to developed countries. There is good evidence to suggest that Indian rural data may be as good as developed country settings when proper operational procedures are followed and good quality devices are used.
- It is possible to closely predict the expected fingerprint recognition performance. In the experiments, it is observed that, at 95% confidence, DB2 is expected to show lower accuracy compared to the Western data whereas DB3 is expected to achieve similar accuracy (for Q = 1, 2, and 3, 99% TAR with about 1% FAR).

- It is believed that DB3's improved image quality is due to better operational procedures. A few simple methods were used in DB3 data collection, such as:
  1. Using wet towels to remove dirt and moisten dry fingers
  2. Using minimum quality threshold to ensure that extra efforts are made to capture good prints from hard to obtain fingers and
  3. Keeping scanning devices in operational order

  These resulted in exceptionally good bin 1 and 2 distribution.
- It is also observed that the slap fingerprint segmentation tools require some prior training for Indian databases. After some training, segmentation results improve by 2-3%. This also suggests that in deploying a biometrics (fingerprint) system, a carefully designed a priori training set and procedure will help in improving performance.
- Since NFIQ tool is trained using Western data, there are around 4-5% errors in correctly assigning the quality scores in the Indian fingerprints. It might be possible to tune the tool to Indian data.
- When the fingerprint images in DB1 (rural and urban setting), specifically those causing errors were analyzed, it was found that there are some specific causes that are more relevant in the Indian sub-continental region compared to Western and European countries. Lawsonia Inermis (commonly known as henna or mehandi) can cause significant differences in the quality of fingerprint images. Widely used by women in the Indian sub-continent during festivals, henna is applied on hand/fingers and when applied, fingerprint sensors may not properly capture fingerprint features.
- On analyzing the quality distribution of each finger in every age group, it is difficult to generalize little fingers as useful or not. Similarly, it is not possible to generalize that, a particular age group or gender conforms to lower or higher quality scores and hence better/worse performance.

Finally, it is strongly recommended that carefully designed experiments and proper statistical analysis under pilot should be carried out, to formally predict the accuracy of biometric systems for Indian rural and urban environments.

Face identification

Face image, uncorrelated to fingerprint image, can be utilized in two ways. Face image can be independently matched using automatic matching algorithm and the results fused together to achieve higher net accuracy. NIST reports improved accuracy using fingerprint and face image score fusion [28]. It should be noted that face image alone provides low accuracy rate. A more practical method is hierarchical matching where false match rate can be improved by comparing face images of suspected duplicates obtained in fingerprint matching. In the former, the entire database has to be used as gallery, making the matching prohibitively expensive. In the later, gallery size is small, typically 1% of database. The hierarchical method improves FRR (which reduces manual duplicate check) but does not directly improve FAR (which results in duplicates in the database). However, one can trade off FRR to improve FAR.

Iris

Iris has been shown to provide accuracy comparable to fingerprint. NIST Iris test provided accuracy rates shown in Figure 24[10]. T. Mansfield of National Physical Laboratory [33] reports low FAR for small sample.

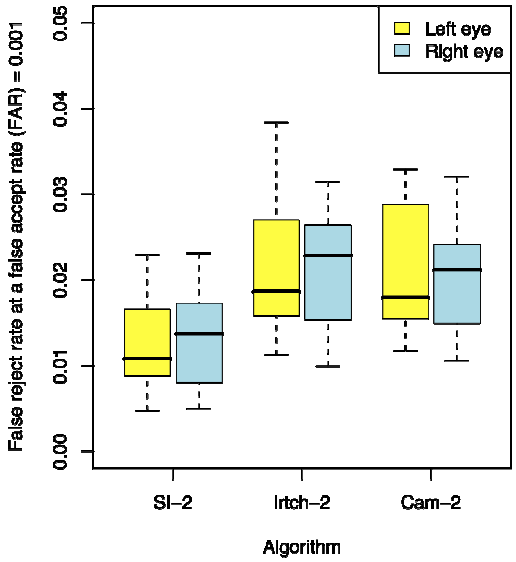

Figure 24 Iris FAR & FRR rate

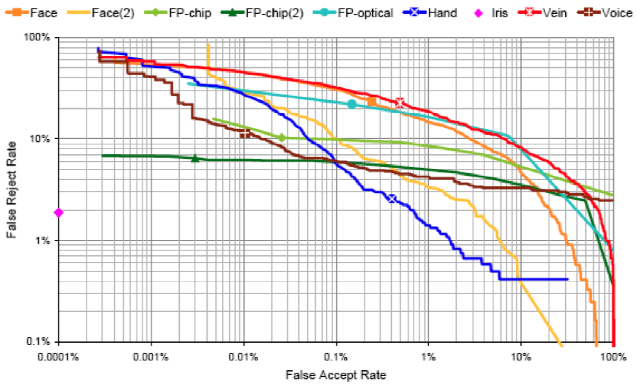

Figure 25 FAR and FRR of various biometric identifier

Fused Accuracy

A large body of literature documents the benefits of information fusion in a variety of fields including search, data mining, pattern recognition, and computer vision. Fusion in biometric is an instance of information fusion. A strong theoretical base as well as numerous empirical studies has been documented that support the advantages of fusion in biometric systems [1]. The main advantage of fusion in the context of biometrics is an improvement in the overall matching accuracy. Depending on the fusion method, the matching speed may also be improved significantly. Dr. Phalguni Gupta and his team report a study of fusion of fingerprint with iris [7]. They show a substantial improvement in matching accuracy by combining one iris with one finger. There is no empirical data available for Indian conditions though there is strong theoretical evidence that among all economically and technically feasible biometrics modalities,

combined fingerprint and iris has potential to provide maximum accuracy in Indian conditions.

ISO Documents

Included by reference

ISO/IEC 19794-2:2005. Biometric data interchange formats – Part 2: Finger minutiae data

ISO/IEC 19794-4:2005. Biometric data interchange formats – Part 4: Finger Image data

ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face Image data

ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris Image data

References

1. A. A. Ross, K. Nandakumar, A. K. Jain, Handbook of Multibiometrics, Springer, 2006
2. Anil Jain, Patrick Flynn, Arun Ross. Handbook of Biometrics, 2008
3. ANSI/NIST-ITL 1-2007. American National Standard for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 1
4. ANSI/NIST-ITL 2-2008. American National Standard for Information Systems—Data Format for the Interchange of Fingerprint, Facial, & Other Biometric Information – Part 2 XML Version
5. Bolle, Connell et al. Guide to Biometrics, 2004
6. Fingerprint Image Data Standards for Indian e-Governance Applications, Draft Version 0.4, National Information Center
7. H. Mahrotra, A. Rattani, P. Gupta, "Fusion of Iris and Fingerprint Biometric for Recognition", Proceedings of International Conference on Signal and Image Processing (ICSIP 2006), Karnataka, India, 2006
8. IAFIS-IC-0100 (V7) Electronic Fingerprint Transmission Standard (EFTS) 1999
9. International Biometrics Group, "Independent Testing of Iris Recognition Technology, Final Report, May 2005", NBCHC030114/0002. Study commissioned by the US Department of Homeland Security.
10. IREX I, "Performance of Iris Recognition Algorithms on Standard Images", NIST Interagency Report 7629
11. ISO/IEC 19784-1:2006. Biometric Application Programming interface – Part1: BioAPI specification.
12. ISO/IEC 19794-1:2006. Biometric data interchange formats – Part 1: Framework
13. ISO/IEC 19794-5:2005. Biometric data interchange formats – Part 5: Face image data
14. ISO/IEC 19794-6:2005. Biometric data interchange formats – Part 6: Iris image data
15. J. Cambier, "Iridian Large Database Performance", Iridian Technical Report 03-002
16. J. Daugman, "Algorithms, Performance & Challenges", BYSM, 2006
17. J. Daugman, "Iris recognition border crossing system in the UAE", International Airport Review (2) 2004.
18. J. Daugman, Technical Report 635, University of Cambridge, 2005
19. James Matey, "Iris Recognition", Sarnoff Corporation, BCC 2005
20. Jonathon Phillips, "ICE 2006 Large-Scale Results", NIST 7208, NIST, 2007
21. NISTIR 7110. Matching Performance for the US-VISIT IDENT System Using Flat Fingerprints. C. L. Wilson, M. D. Garris, & C. I. Watson, May 2004
22. NISTIR 7112. Studies of Plain-to-Rolled Fingerprint Matching Using the NIST Algorithmic Test Bed (ATB). Stephen S. Wood & Charles L. Wilson, April 2004
23. NISTIR 7123. Fingerprint Vendor Technology Evaluation 2003: Summary of Results and Analysis Report, Charles Wilson etc al.
24. NISTIR 7151. August 2004 Fingerprint Image Quality
25. NISTIR 7201. Effect of Image Size and Compression on One-to-One Fingerprint Matching. C. I. Watson & C. L. Wilson. February 2005

26. NISTIR 7249. Two Finger Matching With Vendor SDK Matchers. C. Watson, C. Wilson, M. Indovina & B. Cochran. July 2005
27. NISTIR 7296. MINEX. Performance and Interoperability of the INCI TS 3 7 8 Fingerprint Template. Patrick Grother, Michael McCabe et al. March 2006
28. NISTIR 7346 TR. Studies of Biometric Fusion, 2007
29. Patrick Grother, Elham Tabassi, "Performance of Biometric Quality Measures", IEEE transactions on pattern analysis and machine intelligence, Vol. 29, No. 4, April 2007.
30. Registry of USG Recommended Biometric Standards, Version 2.0, NSTC
31. Report of the working group on standards for raw images of fingerprints, Reserve Bank of India
32. Shahram Orandi, Mobile ID Device Best Practice Recommendations, NIST Special Publication 500-280, August 2009
33. T. Mansfield, G. Kelly, D. Chandler, J. Kane, "Biometric Product Testing Final Report", CESG Contract X92A/4009309, Centre for Mathematics & Scientific Computing, National Physical Laboratory, Queen's Road, Teddington, Middlesex TW11 0LW
34. UK Passport Service, Biometrics Enrolment Trial, May 2005