

Government of India
Ministry of Communications and Information Technology
Department of Information Technology
Electronics Niketan
6, CGO Complex

New Delhi-110003
November 12, 2010

Notification

Standards for Face Image, Fingerprint Image and Minutiae

No. 2(32)/2009-EG-II. WHEREAS, Department of Information Technology (DIT), Ministry of Communications and Information Technology, Government of India (GoI) is driving the National e-Governance Plan (NeGP), which seeks to create the right Governance and institutional mechanism; implement a number of Mission Mode Projects at the Centre & State government and also promote the usage of Open Standards to avoid any technology lock-ins

AND WHEREAS, Standards in e-Governance is considered priority activity, which will help ensure sharing of information and seamless interoperability of data across e-Governance applications and also creation of an Institutional Mechanism under NeGP to evolve/adopt Standards for e-Governance

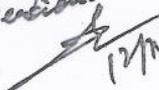
AND WHEREAS, immediate need has been felt to have Standards for identification and authorization of an individual based on his biometrics data like Face image, Fingerprint image and Minutiae

AND WHEREAS, the Competent Authority on Standards has approved the Biometrics Standards for Face image, Fingerprint image and Minutiae based on the ISO 19794 part 5 (Face Image), part 4(Fingerprint Image) and part 2 (Minutiae) standards

NOW, this Department hereby notifies Face image, Fingerprint image and Minutiae Standards for e-Governance Applications w.e.f the date of notification. The Standards can be downloaded from <http://egovstandards.gov.in>.


(S.S. Rawat)
Joint Director

To ✓
The Manager
Government of India Press
Faridabad (Haryana)

✓ Issued Through Speed Post.
with Hindi Version.

12/11/10

: Alongwith Hindi Version.

ofc

Copy for information to:

1. All Secretaries, Government of India
2. Chief Secretaries of all the State Governments
3. Secretary (IT) of all the States.


(S.S. Rawat)
Joint Director

भारत सरकार
संचार और सूचना प्रौद्योगिकी मंत्रालय
सूचना प्रौद्योगिकी विभाग
इलेक्ट्रॉनिक्स निकेतन
6, सीजीओ कॉम्प्लेक्स

नई दिल्ली
12 नवम्बर, 2010

अधिसूचना

मुख चित्र, अंगुलीछाप चित्र और सूक्ष्म चित्र के लिए मानदण्ड

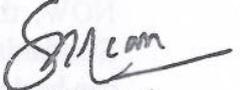
सं. 2(32)/2009-ईजी-॥ जबकि, सूचना प्रौद्योगिकी विभाग, संचार और सूचना प्रौद्योगिकी मंत्रालय, भारत सरकार राष्ट्रीय ई-शासन योजना (इनईजीपी) चला रहा है, जिसमें सही शासन और संस्थागत तंत्र की स्थापना करने, केन्द्र और राज्य सरकार में कई मिशन मोड परियोजनाएँ कार्यान्वित करने की बात की गई है

और जबकि, ई-शासन के मानदण्डों को प्राथमिकता प्राप्त कार्यकलाप माना गया है, जिससे सूचना के आदान-प्रदान और ई-शासन अनुप्रयोगों में डेटा के अविच्छिन्न अन्तर-प्रचालन में तथा ई-शासन के लिए मानदण्ड बनाने/अपनाने के लिए एनईजीपी के अंतर्गत संस्थागत तंत्र की स्थापना करने का भी सुनिश्चय करने में सहायता मिलेगी

और जबकि, किसी व्यक्ति के जैव सांख्यिकी डेटा जैसेकि मुख चित्र, अंगुलीछाप चित्र और सूक्ष्म चित्र पर आधारित उसकी पहचान और प्राधिकरण के लिए मानदण्ड बनाने की तत्काल आवश्यकता महसूस की गई है।

और जबकि, मानदण्ड संबंधी सक्षम प्राधिकारी ने आईएसओ 19794 भाग 5 (मुख चित्र), भाग 4 (अंगुलीछाप चित्र) तथा भाग 2 (सूक्ष्म चित्र) मानदण्डों पर आधारित मुख चित्र, अंगुलीछाप चित्र और सूक्ष्म चित्र के जैव सांख्यिकी मानदण्डों को अनुमोदित कर दिया है।

अब, यह विभाग एतद्वारा अधिसूचना की तारीख से ई-शासन अनुप्रयोगों के लिए मुख चित्र, अंगुलीछाप चित्र और सूक्ष्म चित्र के मानदण्डों को अधिसूचित करता है। इन मानदण्डों को <http://egovstandards.gov.in> से डाउनलोड किया जा सकता है।

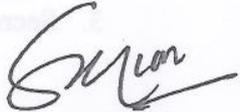

(एस.एस.रावत)
संयुक्त निदेशक

सेवा में,

प्रबंधक
भारत सरकार प्रेस
फरीदाबाद (हरियाणा)

सूचनार्थ प्रतिलिपि :

1. भारत सरकार के सभी सचिव।
2. सभी राज्य सरकारों के मुख्य सचिव।
3. सभी राज्यों के सचिव (सूचना प्रौद्योगिकी)।


(एस.एस.रावत)
संयुक्त निदेशक

eGov.BIDS:01
Version: 1.0
November, 2010

Face Image Data Standard
for
e-Governance Applications in India



Government of India
Department of Information Technology
Ministry of Communications and Information Technology
New Delhi – 110 003

Contents

1. Introduction	1
1.1 Scope	1
1.2 Objective/Purpose	2
1.3 Applicability	2
1.4 Description	2
2. Target Audience	3
3. Type of Standard Document	3
4. Definitions and Acronyms	3
5. Face Image Specifications	4
5.1 Face Image Capturing Device Characteristics.....	4
5.1.1 Source Type.....	4
5.1.2 Pixel Aspect Ratio of the capturing device.....	4
5.2 Face Image Specifications	5
5.2.1 Face Image Type.....	5
5.2.2 Color Space	5
5.2.3 Inter-eye Distance.....	5
5.2.4 Pose Angle.....	5
5.2.5 Shoulders.....	5
5.3 Scene Requirements	5
5.3.1 Expression	5
5.3.2 Background of Face Image	5
5.3.3 Subject and Scene Lighting.....	5
5.3.4 Shadows over the Face.....	6
5.3.5 Shadows in Eye-Socket.....	6
5.3.6 Hot Spots	6
5.3.8 Eye Glasses.....	6
5.4 Photograph Size Specifications for Scanning	6
5.4.1 Width	6
5.4.2 Height.....	6
5.4.3 Aspect Ratio.....	6
5.4.4 Head Width	6
5.4.5 Head Height.....	6
5.5 Face image Capture, Storage and Transmission Formats	7
5.5.1 Image Capturing Format for Enrolment.....	7
5.5.2 Image Capturing Format for Verification	7
5.5.3 Image Storage/Archival Format.....	7
5.5.3.1 Storage / Archival Format for Normal Memory Devices	7
5.5.3.2 Storage Format for Restricted Memory Devices.....	7
5.5.4 Transmission Format for Verification	7
5.5.4.1 Normal Bandwidth	7
5.5.4.2 Restricted Bandwidth.....	8
5.5.5 Transmission Format for Storage / Archival.....	8
5.5.5.1 For Normal Memory Devices.....	8
5.5.5.2 For Restricted Memory Devices	8
5.6 Face Image Record Format Specifications	8
5.6.1 CBEFF Header	8
5.6.2 Facial Record Header.....	8
5.6.3 Facial Record Data	9

5.6.3.1 Facial Information	9
5.6.3.2 Feature Points	9
5.6.3.3 Image Information.....	9
5.6.3.3.2 Image Data Type	9
5.6.4 CBEFF Signature.....	9
6. Best Practices	10
6.1 Best Practices for Implementation of Standard Specifications	10
6.2 Quality Check List.....	13
6.3 Face Image Record Format Values	14
6.3.1 Facial Record Header.....	14
6.3.2 Facial Record Data	14
6.3.3 Facial Information block.....	15
6.3.4 Image Information.....	16
6.4 Operational Instructions for Image Acquisition	17
6.4.1 Process of Enrolment	17
6.4.1.1 Process at Client end	17
6.4.1.2 Process at Server end.....	17
6.4.2 Process for Human Visual Inspection and Verification	17
7. Annexure	18
Annexure-I Definitions and Acronyms	18
8. References	21
9. List of Contributors	22

1. Introduction

The Indian Government proposes to use biometric data for identification and verification of individuals in e-Governance applications. The biometric data includes fingerprint image, minutiae, face image and iris data.

This standard deals with usage of face image data for human visual inspection and verification.

With the objective of interoperability among various e-Governance applications, the face image data standard for Indian e-Governance Applications will adopt ISO /IEC 19794-5:2005(E). While the ISO standard is broad to cover all possible applications of computer based face recognition and human visual inspection, this standard is more restrictive, as it is limited to human visual inspection. However, this standard does consider the future use of the stored face images for computer based facial recognition. The ISO standard specifications are tailored to meet specific needs of civilian e-Governance applications by specifying certain prescriptive values and best practices suitable in Indian context.

1.1 Scope

This standard includes capture and storage specifications of face images for human visual inspection and verification of the individuals in Indian E-Governance applications. A possible future use of these images for computer based face recognition is kept in view during the capture and storage. It specifies a format to store face image data within a biometric data record compliant to the Common Biometric Exchange Formats Framework (CBEFF), given in ISO 19785-1. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications.

The Indian e-Governance applications will have both biometric identification and verification phases, to ensure there is no duplication of identity and to verify the identity of a person for access to the services of the application. The face image would be mainly used for verification of identity of an individual along with other biometric data like fingerprints/iris image data. In case of missing fingerprints/iris data of an individual, it would be used as primary data for identification/verification.

Manual Facial recognition is not sufficient currently for de-duplication.

. Computer based face recognition has reasonable accuracy under controlled conditions only. Hence for de-duplication purposes, other biometrics like finger print/iris image are also recommended which are beyond scope of this document.

In view of the above, the scope of this standard includes:

- a. Characteristics of Face Image capturing device
- b. Specifications of Digital Face Image & Face Photograph Specifications intended only for human visual inspection and verification
- c. Scene requirements of the face images, keeping in view a future possibility of computer based face recognition

- d. Face Record Format for storing, archiving, and transmitting the information of face image within a CBEFF header data structure for the purpose of interoperability and usage in future for computer based face recognition.

This standard is sufficiently broad to cover the requirements of all e-Governance applications. The applications may judiciously select the specifications relevant to their needs.

1.2 Objective/Purpose

The purpose of this standard is to provide the capture and storage specifications of face images to ensure capture of good quality image and interoperability in Indian e-Governance applications. The specifications are mandated where necessary or recommended as best practices, where possible.

The intended applications are:

- a. **Human visual inspection** of facial images with sufficient resolution to allow a human (manual) examiner to ascertain small features such as moles and scars that might be used to verify a person's identity.
- b. **Human (manual) verification of identity** by comparison of a person's face against his/her stored facial image.

1.3 Applicability

These biometric Standards would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards.

1.4 Description

Photograph of the face is commonly used in various types of identification cards and there is wide public acceptance for this biometric identifier. Photograph stored in digital form/electronic representation of portrait i.e. face image, can be used either for display for human visual inspection or for computer based face recognition.

As per ISO/IEC 19794-5 Face Image Data standard, there are mainly two types of face images as follows:

Basic face image: It specifies face image record format including header and image data. It is a fundamental requirement of face image acquisition.

Frontal Image: It is a basic face image that adheres to additional requirements appropriate for frontal face recognition and/or human examination.

There are two types of Frontal Face Images - Full Frontal & Token Frontal as described below:

Full Frontal Type: It specifies frontal image with sufficient resolution for human examination as well as reliable computer based recognition. This image includes the full head width, all hair in most cases, as well as neck and shoulders. This image type is suitable for permanent storage of the face information, and it is applicable to portraits for passport, driver license, and other ID cards.

Token Frontal: A face image type that specifies frontal images with a specific geometric size and eye positioning based on the width and height of the image. This image type is suitable for minimizing the storage requirements for computer face recognition tasks such as verification while still offering vendor independence and human verification capabilities.

A face needs to be well lighted using controlled light sources, and in frontal pose for visual examination or automated recognition. There are many other technical challenges also associated with robust face recognition, which can be addressed by following standard specifications and recommended best practices.

This version of the Face Image Standard describes standard specifications and recommended best practices focused around Frontal Image, which inherits basic image requirements also.

2. Target Audience

All e-Governance projects rolled out by Central and State Governments or any other organization using face images or face photographs.

Photographers, who capture facial images for e-Governance applications.

All Integrators/Biometric Service providers.

3. Type of Standard Document

Type: Standard Specifications & Best Practices

Enforcement Category:

Standard Specifications – Mandatory

Best Practices: Recommended

4. Definitions and Acronyms

Refer Annexure I

5. Face Image Specifications

In the present version of the Standard, the face images are intended only for human (manual) verification in Indian e-Governance applications. These images are mandated to be frontal face images with standard specifications in compliance with International standard ISO 19794-5: 2005(E). Latest technical amendments/enhancements issued by ISO over this standard are being examined, for future versions of this standard.

In order to be interoperable among different vendors, it is required that these images be stored in a format compliant to the international standard ISO 19794-5, within the overall Common Biometric Exchange Formats Framework (CBEFF) as per ISO 19785-1.

The standard specifications are divided into five components as follows:

- a. Face Image capturing Device Characteristics
- b. Face Image and Photograph Specifications
- c. Scene requirements
- d. Face image Capture, Storage and Transmission Specifications
- e. Face Image Record Format Specifications.

5.1 Face Image Capturing Device Characteristics

5.1.1 Source Type

- a. Static face image from a **Digital still image camera or Web camera (0x02)** which supports image capturing in a format as specified in section 5.5 and having specifications to meet the image quality requirements.

Refer section 6.1.1(a) for best practices for certain device specifications.

- b. Digitized photograph from a flatbed **Scanner (0x03)** of 118 dpcm (300 dpi) resolution that supports image capturing in a format as specified in section 5.5

Note: Scanner specifications require much more detailing like scanner type, quality requirements, speed etc. In view of the fact that presently many Governance applications may require to use scanner, the present version includes minimum required specifications for scanner. Detailed specifications are being worked out which would be released soon through a corrigendum.

Refer section 6.1.1(b) for best practices.

Refer section 5.7.6 of ISO 19794-5:2005 (E) for the source type codes.

5.1.2 Pixel Aspect Ratio of the capturing device

Pixel aspect ratio should be 1:1

5.2 Face Image Specifications

5.2.1 Face Image Type

The Full Frontal Image should be captured as per the specifications laid down in this Standard.

Refer section 8.3 of ISO 19794-5 for more detailing about photographic requirements of full frontal face image type

Refer section 6.1.5 for recommended best practices for full frontal image specifications for travel documents

5.2.2 Color Space

24 bit RGB (i.e. Code 0x01)

Refer section 5.7.5 and Table 12 of ISO/19794-5.

5.2.3 Inter-eye Distance

The Inter-eye distance should be a minimum 120 pixels for a head width of 240 pixels.

Refer section A.3.1 of ISO 19794-5.

Refer section 6.1 for recommended best practices.

5.2.4 Pose Angle

Rotation of the head shall be less than ± 5 degrees from frontal in every direction (i.e. roll, pitch and yaw).

5.2.5 Shoulders

Both the shoulders should be visible.

5.3 Scene Requirements

5.3.1 Expression

Expression of the face should be neutral (non-smiling) with both eyes open normally (i.e. code 0x01). This information has to be stored in the facial image header because it would help in automatic face recognition in the future.

5.3.2 Background of Face Image

White background is recommended, provided there is sufficient distinction between the face/hair area and the background. In situations where distinction is not clear, a light gray background, up to **18% gray level** is permitted.

Only one person should be present in the photograph and no other person or object should be present in the background covered in the face image.

5.3.3 Subject and Scene Lighting

Natural lighting should be equally distributed on the face

Refer section 7.2.7 of ISO 19794-5:2005(E).

5.3.4 Shadows over the Face

The region of the face, from the crown to the base of the chin and from ear-to-ear, shall be clearly visible and free of shadows (*Refer section 7.2.8 of ISO 19794-5:2005(E)*).

5.3.5 Shadows in Eye-Socket

There shall be no dark shadows in the eye-sockets due to the brow. The iris and pupil of the eyes shall be clearly visible (*Refer section 7.2.9 of ISO/19794-5*).

5.3.6 Hot Spots

Care should be taken to avoid hot spots (bright areas of light shining on the face (*Refer section 7.2.10 of ISO 19794-5:2005(E)*)).

5.3.8 Eye Glasses

Glasses should be clear and transparent to ensure clear visibility of eye pupils and irises.

Note: Quality of face image will be checked based on the above specifications. A complete checklist is provided in the best practices section 6.2. The face image will get qualified for storage at the time of enrolment or manual verification, only if it clears all the checklist features.

5.4 Photograph Size Specifications for Scanning

Photograph to be scanned for digitization should adhere to specifications of the face image & scene requirements mentioned above. In addition, it should have the following size specifications:

5.4.1 Width

The width of the face photograph should be approximately 35 mm (1.4 inches).

5.4.2 Height

The height of the face photograph should be approximately 45 mm (1.75 inches).

5.4.3 Aspect Ratio

Width to height ratio should be between 1:1.25 – 1.33

5.4.4 Head Width

The head width of the face in the photograph should be approximately 20 mm (0.79 inches). The head width relative to photograph width should be between 50% to 70%.

5.4.5 Head Height

The head height (chin to crown portion) of the face in the photograph should be approximately 25 mm (0.98 inches). Head height relative to photograph height should be between 70% to 80% .

Refer section A.3.1 of ISO 19794-5 for these specifications.

5.5 Face image Capture, Storage and Transmission Formats

5.5.1 Image Capturing Format for Enrolment

For enrolment, the face image can be captured in lossless format (PNG/ JPEG¹2000/ DNG/ TIFF/ RAW).

5.5.2 Image Capturing Format for Verification

For human manual inspection, usually the verification is done by comparing the face of person with printed photograph on the travel document / identity card. However, at times, there may be a need to capture image of the face for verification. Depending upon the e-Governance application sensitivity requirements, the face image for verification can be captured either in lossless format (PNG/ JPEG2000/ DNG/ TIFF/ RAW) or JPEG2000² with compression ratio up to 1:15.

5.5.3 Image Storage/Archival Format

Once the face image gets qualified after quality check, it needs to be retained/stored/transmitted. The data storage/transmission format specifications should adhere to the Policy on Open Standards to ensure interoperability, vendor independence, long-term availability of data and optimal utilization of storage space, without affecting the quality of the image.

The storage of the image in normal memory devices like client /server systems or restricted memory devices like smart card would be done in the face record format as described in section 5.6.

5.5.3.1 Storage / Archival Format for Normal Memory Devices

PNG format (*compression algorithm code 5 as per table 3 of ISO 19794-4: 2005(E)*)

The example of such device is Desk top client / Server.

Note: The image should never undergo any lossy compression at any stage from the instant of capture to storage in database.

5.5.3.2 Storage Format for Restricted Memory Devices

JPEG2000 with compression ratio up to 1:15 (*compression algorithm code 4 as per table 3 of ISO 19794-4: 2005(E)*)

The examples of such devices are Smart card, mobile phones etc.

5.5.4 Transmission Format for Verification

5.5.4.1 Normal Bandwidth

PNG

¹ The usage of term JPEG 2000 in this document means JPEG2000 part- 1 (for static/still image) , or JPEG2000 Basic or JPEG2000 Core Coding System, or ISO/IEC-15444-1

5.5.4.2 Restricted Bandwidth

JPEG2000 with compression ratio up to 1:15

5.5.5 Transmission Format for Storage / Archival

5.5.5.1 For Normal Memory Devices

The face image captured during the enrolment process should be transmitted in **lossless** format (PNG/ JPEG³2000/ DNG/ TIFF/ RAW) from client system to the server for storage / archival in the standardized format for future usage.

5.5.5.2 For Restricted Memory Devices

Face image can be transmitted in JPEG2000 format with compression ratio up to 1:15.

5.6 Face Image Record Format Specifications

This is a format to store face image data within a biometric data record to cater to interoperability requirements of the face image taken by various image acquisition devices. It also stores specific information related to the face image, which would be useful in future automatic verification of face images.

CBEFF (Common Biometric Exchange Formats Framework) described in ISO 19794-5 will be adopted. This format is based on ISO 19785-1.

The Face Image Record Format is broadly structured as follows:

- a. CBEFF Header
- b. Facial Record Header
- c. Facial Record Data (Facial Information, Feature points, Image Information, Image Data)
- d. CBEFF Signature (This is optional as it is used for encrypting & digitally signing the data wherever required).

The format is described below, and for best practices *refer section 6.3*

5.6.1 CBEFF Header

A Standard Biometric Header (SBH) with values, as prescribed in ISO 19785-1 will be stored.

5.6.2 Facial Record Header

It has fixed 14 bytes length containing information about the overall record of face image like format identifier (4 bytes), version no (4 bytes), length of record (4 bytes), number of face images (2 bytes). In format Identifier, the value will be 0x464114300 ('F' 'A' 'C' 0x0), version

³ The usage of term JPEG 2000 in this document means JPEG2000 part- 1 (for static/still image) , or JPEG2000 Basic or JPEG2000 Core Coding System, or ISO/IEC-15444-1

number for this standard will be 0x30313000 ('0' '1' '0' 0x0), length of the record includes Facial Record Header and Facial Record Data. Number of face images for this standard is 1.

5.6.3 Facial Record Data

ISO 19794-5:2005(E) specifies that the Facial Record Data contains Facial Information, Feature point(s), Image Information and Image Data as detailed below:

5.6.3.1 Facial Information

The Facial Information Block of fixed 20 bytes contains fields of Facial Record Data length, Number of Feature points, and additional fields to specify gender, eye color, hair color, property mask, expression, pose angle, pose angle uncertainty. Specifying values for additional fields would be optional. In such cases, the default values would be taken as "Unspecified (Code 0x0)"

The feature points are optional in the ISO 19794-5 standard and hence their storage are not required as per this standard as only manual verification is considered here. Therefore, the value of 'Number of feature points' in the Facial Information field would be "0x0" (2 bytes). The values of facial information like gender, eye color, hair color, property mask, expression, pose angle, pose angle uncertainty will have to be entered corresponding to the captured image.

5.6.3.2 Feature Points

Since the current version of this standard caters to manual verification only, feature points are not stored.

5.6.3.3 Image Information

The value of image information like face image type, image data type, width, height, image color space, source type, device type, will have to be entered corresponding to the captured image.

5.6.3.3.1 Face Image Type

This standard will store face images in Full Frontal Image type (0x01).

5.6.3.3.2 Image Data Type

The Image Data type represents the compression formats of the stored face image.

Refer section 5.5.3 for compression types for storage of image data on different types of devices.

5.6.4 CBEFF Signature

This is optional as it is used for encrypting and digitally signing the image data, wherever required.

Note: Refer section 6.3 for CBEFF detailed structure and the prescribed values tailored to Indian e-Governance applications requirements.

6. Best Practices

The e-governance standards are intended for a variety of e-Governance application with varying degree of sensitivity and volume.

The specifications in Section 5 are broad in nature to cater to all types of e-Governance applications requirements. This Section covers recommended best practices suitable for various categories of applications.

6.1 Best Practices for Implementation of Standard Specifications

6.1.1 Device Specifications & Operational Instructions

Refer section 5.1.1 for
Source Type specifications

a. Source type: Digital camera / Web camera

- i. It should strictly meet the specifications requirements of the standard
- ii. Since the captured face images are to be archived for automatic face recognition in future, it is recommended that for enrolment, preference should be given to Digital Single Lens Reflex (DSLR) or mid range digital point-and-shoot camera
 or
 High end web camera (without any artifacts and fish-eye effect), where output is similar to a digital camera.

Operational Instructions

- i. Preference should be given to the use of tethered digital camera / web camera along with APIs to have direct link with computer for image transfer and on line quality check etc, while capturing the face image
- ii. The attributes of the camera should be adjusted to meet the standard specifications. Under no circumstances, zoom option of the camera should be used
- iii. The vendor should ensure appropriate lighting conditions to meet the quality requirements
- iv. In a typical enrolment setup, the camera will be connected to a computer for online checking of quality of facial image, as per the defined parameters listed in Quality Check list at section 6.2, and for conversion of the image into the desired storage formats.

Refer section 6.4 for more detailed operational instructions for acquisition of face images for enrolment /verification.

	<p>b. Source Type: Scanner</p> <p>Before scanning the photograph, one should ensure that the paper photograph to be scanned meets the standard specifications of full frontal image</p> <p>Note: Preference should be given to the use of digital camera / web camera with desirable device specifications for capturing the face images</p>
<p>6.1.2 Face Image Specifications</p>	
<p><i>Refer section 5.2.1 for</i> Face Image Type specifications</p>	<p>The full frontal images are required for human visual inspection as-well-as travel documents like Passport, Driver Licenses, identity cards etc.</p> <p>The digital camera / web camera should be positioned appropriately to ensure that specifications mentioned in Section 5.2 are met.</p>
<p><i>Refer section 5.2.3 for</i> Inter Eye Distance specifications</p>	<p>Inter eye distance specifications can be ensured by different processes such as:</p> <ul style="list-style-type: none"> i. Adjusting the distance between the person and camera ii. Manual measurement of the distance between the eyes iii. Automatic eye location and inter eye distance computation on digital face images.
<p>6.1.3 Scene Requirements</p>	
<p><i>Refer section 5.3 for</i> Scene requirements</p>	<p>Vendor to certify the quality of the face image by filling check list given in Section 6.2 <i>Refer ISO 19794-5: 20005(E) Section A.3.2.4 for more details. An illustration of acceptable quality of full frontal face image</i></p> <div data-bbox="587 1429 837 1727" style="text-align: center;">  </div>

6.1.4 Face Image Capture and Storage Requirements	
<i>Refer section 5.5 for</i> Face image capture and storage requirements	<p>For Enrolment Default face image type for storage is “Full Frontal”. However, in case of resource constraints with respect to storage space, option of storing face image using Token Frontal type can be considered.</p> <p><i>Refer section 9.2.3 of ISO 19794-4:2005(E) for detailing of token image</i></p>
6.1.5 Use of Full Frontal image for Travel Documents	
<i>Refer sections 5.2 & 5.4 for</i> face image & photograph specifications	<p>Width of face Image The width of the face image should be a minimum of 420 pixels. <i>Refer section A.3.1 of ISO 19794-5.</i></p> <p>Height of face Image The height of the face image should be a minimum of 525 pixels. <i>Refer section A.3.1 of ISO 19794-5</i></p> <p>Width to Height ratio of image It should be between 1:1.25 – 1:1.33</p> <p>Head Width The ratio of head width relative to width of the face image should be between 5:7 and 1:2.</p> <p>Head Height The head height (chin to crown portion) of the full face frontal pose should occupy 70% to 80% of the vertical height of the face image</p>
6.1.6 Use of Full Frontal image / Photograph for Identity Cards	
<i>Refer section 5.2.2 for</i> photograph specifications	<p>The printed full frontal face images are used in ID cards, passports, driving licenses and other documents.</p> <p>Note: The printing size mentioned in section 6.1.5 is recommended for consideration for standardization, which is beyond the scope of this standard.</p>

6.2 Quality Check List

Quality check list, as per the specifications & the best practices in Sections 5 and 6.1 5.

S.No.	Parameter & Prescriptive values	Yes	No
01	Visual clarity of the output image (no motion blur, no over or under exposure, no un-natural color, proper and equally distributed lighting with no shadows over the face, no shadows in eye sockets, no hot spots, no radial distortion and no fish-eye effect)		
02	Photo taken within 6-months (for enrolment)		
03	Pixel resolution for digital camera or web camera – minimum 118 ppcm(300 ppi) / Scan resolution for scanner minimum approximately 118 dpcm (300dpi)		
04	Size (width approximately 35 mm (1.4 inches) & Height 45 mm (1.75 inches)) in case of scanned photograph		
05	Outline of the shoulders Visible		
06	Showing white or light gray (18%) background color		
07	Background plain (No other objects in the background)		
08	Chin to crown clearly visible		
09	Head coverage of the person minimum 80%		
10	Neutral expression (mouth closed, eyes open)		
11	No reflection on Face		
12	Showing both edges (both ears) of the face clearly		
13	Showing the skin tones naturally		
14	Red eye correction done		
15	Inter eye distance minimum 120 pixels		
16	Looking directly at the camera		
17	Eyes open and clearly visible , and not covered with hair or any other obstacle		
18	Clearly visible eyes, in case of wearing spectacles, and no color glasses. (If applicable)		
19	Spectacles not heavy and not covering eyes (if applicable)		
20.	No accessories (Other than turban due to religious reasons, eye patches due to medical reasons supported by medical certificate, small nose ring)		

6.3 Face Image Record Format Values

Refer section 5.5 for Face image record format specifications

- a. Values in **shaded rows** are variable in nature and need to be entered on case- to **case basis**
- b. Values in other rows are fixed in nature as per ISO 19794-5:2005(E) specifications and should not be altered.

6.3.1 Facial Record Header

(Format and fixed values extracted from ISO 19794-5:2005(E))

Field	Size	Value
Format Identifier Indicates face image data	4 bytes	0x46414300 (‘F’ ‘A’ ‘C’ 0x0)
Version Number	4 bytes	0x30313000 (‘0’ ‘1’ ‘0’ 0x0)
Length of records (Including length of Facial Record Header and Facial Record Data)	4 bytes	46<Length of Record<=2 ³²⁻¹
Number of facial images	2 bytes	1

6.3.2 Facial Record Data

Prepared based on Figure 2 of ISO19794-5:2005(E)

Field	Size	Value
Facial Information	20 bytes	Details in Table at 6.3.3
Feature Point	N.A	Not stored as the standard is for manual verification only. (This is an optional block in ISO Standard)
Image Information	12 bytes	Details in table 6.3.4
Image Data	Variable	

6.3.3 Facial Information block

Field	Size	Value
Facial Record data length	4 bytes	
Number of feature Points	2 bytes	0x0 (No feature points are stored)
Gender 0x0 – Unspecified 0x01 - Male 0x02 -Female 0x0FF- Transgender (Table 3 of ISO 19794-5)	1 byte	Relevant value to be entered (0x0 would be the default value, if not filled by vendor)
Eye Color 0x0 - Unspecified 0x01 - Black 0x02 -Blue 0x03 - Brown 0x04 – Gray 0x05 – Green 0x06 – Multi-Colored 0x07 – Pink 0x08-0x0FE – Reserved 0x0FF- Other (Table 4 of ISO 19794-5)	1 byte	Relevant value to be entered (0x0 would be the default value, if not filled by vendor)
Hair Color 0x0 - Unspecified 0x01 - Bald 0x02 -Black 0x03 - Blonde 0x04 - Brown 0x05 – Gray 0x06 – White 0x07 – Red 0x08-0x0FE – Reserved 0x0FF- Other (Table 5 of ISO 19794-5)	1 byte	Relevant value to be entered (0x0 would be the default value, if not filled by vendor)
Property Mask 0-Properties are specified 1 Glasses 2 Moustache 3 Beard 4 Teeth visible 5 Blink (either or both eyes closed) 6 Mouth open 7 Left eye Patch 8 Right eye Patch	3 bytes	Relevant value to be entered

9 Dark Glasses (medical)		
10 Feature Distorting Medical condition (which could impact Feature Point detection)		
11-23 Reserved for Future definition (Table 6 of ISO 19794-5)		
Expression	2 bytes	0x01 (Neutral)
Pose Angle	3 bytes	0x0
Pose Angle Uncertainty		0x0

6.3.4 Image Information

Field	Size	Value
Face Image type	1 bytes	0x01
Image Data Type 0x0 uncompressed no bit packing 0x1 – Uncompressed bit packed 0x04 – JPEG 2000 0x02-0xFF – Reserved 0x5 - PNG (Table 3 of ISO 19794-4)	1 bytes	0x05 – PNG for storage in large memory devices /archival 0x04 – JPEG2000 with compression ratio up to 1:15 for storage in low memory devices
Width	2 bytes	Approximately 420 (in pixels)
Height	2 bytes	Approximately 525 (in pixels)
Image color space	2 byte	0x01 (24 bit RGB)
Source Type	1 byte	0x02 (Digital camera/Web cam) 0x03 (Scanner)
Device type (vendor specific captured device type ID) 0x0 Device type not specified	2 bytes	Relevant value to be entered

Quality	2 bytes	Null - Reserved for future use
Facial Image Data		- PNG for enrolment and archival, and JPEG2000 with compression ratio up to 1:15 for verification

6.4 Operational Instructions for Image Acquisition

In the typical enrolment setup, the camera will be connected to a computer for online checking of quality of facial image, as per the defined parameters listed in Quality check -list at 6.2, and conversion of the image into the desired format.

6.4.1 Process of Enrolment

6.4.1.1 Process at Client end

- a. Capture facial Image data through a digital camera /web camera connected with a computer for desired online settings as per standard specifications for acquisition of face image
- b. Do quality check of captured image online as per the standard specifications
- c. Store Facial Image data as per desired specifications along with CBEFF format details in secured manner on client machine along with demographic data of the enrolee, if available
- d. Transmit the image to the server, in its native captured format or lossless compressed format, as per the standard specifications.

6.4.1.2 Process at Server end

- a. Search the relevant record of the person on the basis of Demographic data. Manually verify enrolee's facial image, if already available on the server. In case of mismatch, flag the discrepancy for further enquiry. In case of a match, proceed further
- b. Store / Archive the Facial data of the enrolee in the prescribed format, as per standard specifications, on the server database, in case the data was not found to be on the server earlier, or an update is required.

Note: The image stored for enrolment purpose should never undergo lossy compression at any stage from the instant of capture to storage in database at server.

6.4.2 Process for Human Visual Inspection and Verification

Either visually compare the face of the person with displayed face image, already stored on server / smart card / displayed in the travel document

OR

An application may require capturing of face image in the verification stage for transmission/ record keeping /online manual inspection and verification with already stored image on server /smart card at the time of enrollment. In such cases, the face image would be captured as per standard specifications.

7. Annexure

Annexure-I Definitions and Acronyms

(Source: Various ISO Standards, ICAO Standards, Wikipedia etc.)

Acquisition

Process of accepting a biometric sample(s) in accordance with the defined policy, that is deemed suitable for creating a biometric reference or a biometric probe.

Note: In addition to capture, acquisition may include segmentation, biometrics feature extraction, quality control and other pre-processing steps.

Biometrics

[Automated] recognition of [living] persons based on observation of behavioral and biological (anatomical and physiological) characteristics.

Biometric System

An automated system capable of:

1. Capturing a biometric sample from an end user;
2. Extracting biometric data from that sample;
3. Comparing the biometric data with that contained in one or more reference templates;
4. Deciding how well they match; and
5. Indicating whether or not an identification or verification of identity has been achieved.

Biometric Data

The data representing a biometric characteristic

Note: For the purpose of this document, biometric data refers to Face Image data.

Example: Image data, behavioral data

Biometric Data Block (BDB)

Block of data with a defined format that contains one or more biometric samples or biometric templates

Biometric Sample

Data obtained from a biometric device, either directly or after processing.

Biometric Template

Biometric sample or combination of biometric samples that is suitable for storage as a reference for future comparison

Capture

The process of taking a biometric sample from an end user.

Capture Device type ID

The capture device type ID shall be a unique identifier for the type of capture device deployed to acquire a biometric sample. The capture device type ID shall be recorded in two bytes. A value

of all zeros indicates that the capture device type ID is unreported. The value “unreported” may not be allowable in some applications. The value field is determined by the vendor, possibly depending on requirements for the respective application

Chin

The central forward portion of the lower jaw

Color image

Continuous tone image that has more than one channel, each of which is coded with one or multiple bits

Color space

The way of representing colours of pixels in an image is colour space. For instance, RGB used in this document.

Crown

Top of the head, or (if obscured by hair or headwear), where the top of the head/skull would be if it could be seen

Enrolment

The process of collecting biometrics samples from a person and the subsequent preparation and storage of biometrics reference templates representing that person’s identity.

Enrolee

A human being, whose image is being captured for Enrolment / Verification

Face Image

Electronic image-based representation of the portrait of a person.

Face Image Type

A category of facial images that satisfy specific requirements.

Human (manual) examination

Process of careful human (manual) comparison of a face image with a person or another face image to ascertain the identity of the respective person by a detailed examination of facial features and structures.

Identification

The one-to-many process of comparing a submitted face image against all of the face images on database to determine whether it matches any of the templates and, if so, the identity of the person matched. The biometric system using the one-to-many approach is seeking to find an identity amongst a database rather than verify a claimed identity.

Matching

The process of comparing a biometric sample (face image) against a previously stored template and scoring the level of similarity.

One-to-many

Synonym of “Identification”.

One-to-one

Synonym of “verification”.

JPEG 2000 Part-1⁴

Static/still Image compression standard specified as ISO/IEC 15444-1:2004

Feature Point

Reference point(s) in a face image as used by face recognition algorithms, commonly referred to as a landmark. Example : Position of the eyes.

Photograph

A paper photo of a full frontal face which can be used for digitization through a scanner or printed face image to be used for human visual inspection

Pixel

Picture element; element on a two-dimensional array that comprises an image.

Portrait

A photograph of a person which includes the full head, with all hair in most cases, as well as neck and top of shoulders.

Red-eye

The red glow from subject’s eye caused by light from flash reflecting from blood vessels behind the retina.

Vendor

Digital camera / Web camera /Scanner manufacturer..

Abbreviated Terms

API	Application Programming Interface
BDB	Biometric Data Block
DPCM	Dots per centimeter
DPI	Dots per inch
PPCM	Pixels per centimeter
PPI	Pixels per inch
PNG	Portable Network Graphics

⁴ JPEG 2000 part- 1 (for static/still image) , or JPEG2000 Basic or JPEG2000 Core Coding System mean the same thing

8. References

Normative References

- [1] ISO 19794-5: 2005(E) Information Technology – Biometric data interchange formats – Part 5 Face image data.
- [2] ISO/IEC 19785 (all parts), Information technology — Common biometric exchange formats framework
- [3] ISO/IEC 19794-1, Information technology — Biometric data interchange formats — Part 1: Framework
- [4] ISO/IEC-15444-1 Information technology – JPEG2000 image coding system : Core coding system

Other References

- [1] Biometric Design Standards for UID applications, Version 1.0, December, 2009
- [2] Internal Report from Expert Committee for Mapping Open Standards Principles to Technology Standard of Interoperability Framework for e-Governance(IFEG) for referred image storage formats like uncompressed lossless(uncompressed , PNG) and JPEG2000 for static image
- [3] Government of India's Policy on Open Standards for e-Governance

9. List of Contributors

Expert Committee Contributors

S. No	Name & Designation	Email Address
1.	Professor Manindra Agrawal (Chairman) Department of computer Science & Engineering Indian Institute of Technology (IIT), Kanpur.	manindra@cse.iitk.ac.in 9935062605
2.	Mr. S. K. Sinha (Nodal Officer) Scientist F , NIC, New Delhi	sinha.sk@nic.in
3.	Dr. Mayank Vatsa Assistant Professor, IIIT Delhi	mayank@iiitd.ac.in
4.	Dr. Richa Singh Assistant Professor, IIIT Delhi	rsingh@iiitd.ac.in
5.	Shri G.S. Raghu Raman CMC Limited , Hyderabad	raghuramam.gadepally@cmcltd.com
6.	Mr. R. Ramesh Scientist E , OTC, NIC, Chennai	ramesh@nic.in

Technical Expert on Biometrics

S. No	Name & Designation	Email Address
1.	Dr. Krithika Venkataramani Asst. Professor , IIT Kanpur	krithika@cse.iitk.ac.in
2	Mr. Rajesh Mashruwala Member, UIDAI	mashru@iitbombay.org

Other Contributors

S. No	Name & Designation	Email Address
1.	Mrs. Aruna Chaba Scientist F & Head, e-Governance Standards Division, NIC, New Delhi	chaba@nic.in
2.	Dr. P. Balasubramanian Scientist G & Head OTC, NIC, Chennai	p.balu@nic.in
3.	Ms. Renu Budhiraja, Director (Egov Division), DIT , New Delhi	renu@mit.gov.in
4.	Ms. Anita Mittal Senior Consultant , DIT, New Delhi	am4anitamittal@gmail.com
5.	Dr. Meenakshi Mahajan Scientist E, NIC, New Delhi	meenakshi.mahajan@nic.in
6.	Mr. Rajnish Kumar Sharma Junior Research Fellow, NIC, New Delhi	rajneesh.sharma@nic.in

eGov.BIDS:02
Version: 1.0
November 2010

Fingerprint Image and Minutiae Data Standard
for
e-Governance Applications in India



Government of India
Department of Information Technology
Ministry of Communications and Information Technology
New Delhi – 110 003

CONTENTS

1. Introduction	1
1.1 Scope	1
1.2 Objective/Purpose	2
1.3 Applicability	2
1.4 Description	2
2. Target Audience	3
3. Type of Standard Document	3
4. Definitions and Acronyms	3
5. Specification of Fingerprint Image Standard	3
5.1 Device Specifications & Setting	4
5.2 Image Specifications	5
5.2.1 Impression Type	5
5.2.1.1 Enrolment / Identification	5
5.2.1.2 Verification.....	5
5.2.2 Finger Position.....	5
5.2.2.1 Enrolment / Identification/Verification	5
5.2.3 Rotation Angle	5
5.2.4 Number of Fingers	5
5.2.4.1 Enrolment/ Identification	5
5.2.4.2 Verification.....	5
5.2.5 Fingerprint Acquisition Format.....	6
5.2.5.1 Enrolment	6
5.2.5.2 Verification.....	6
5.3 Quality Specifications	6
5.4 Fingerprint Storage / Archival and Transmission Specifications	6
5.4.1 Storage / Archival Specifications	6
5.4.1.1 Storage / Archival Format for Normal Memory Devices.....	6
5.4.1.2 Storage Format for Restricted Memory Devices	7
5.4.2 Transmission Format for Verification	7
5.4.2.1 Normal Bandwidth	7
5.4.2.2 Restricted Bandwidth	7
5.4.3 Transmission Format for Storage	7
5.4.3.1 For Normal Memory Devices.....	7
5.4.3.2 For Restricted Memory Devices	7
5.5 Minutiae Data Format Specifications	7
5.6 Fingerprint Image Record Format	7
6. Best Practices	9
6.1 Best Practices for Implementation of Fingerprint image Specifications	9
6.2 Best Practices for Various Processes	11
6.2.1 Enrolment Process	11
6.2.2 Verification Process	12
6.2.3 Process for capturing rolled fingerprint images	12
6.3 Fingerprint Record Format Specifications	12
7. Annexure	15
8. References	19
9. List of Contributors	20

1. Introduction

The Indian Government proposes to use biometric data for identification and verification of individuals in e-Governance applications. The biometric data includes fingerprint image, minutiae, face image and iris data.

This standard deals with usage of **fingerprint image data and minutiae data** for identification and verification of an individual.

Fingerprint is an important and unique biometric characteristic of an individual. There are many vendors selling finger print devices for acquisition of the data in different ways. Also various algorithms are available for fingerprint features extraction and matching. It is necessary that these vendors follow fingerprint standards and best practices to ensure interoperability of devices and algorithms to avoid vendor lock-in, and also ensure long term storage of data with technology independence.

For this purpose, the Government of India would adopt ISO/IEC 19794-4:2005(E) as Fingerprint Image standard, and ISO 19794-2:2005(E) as Minutiae data format standard. The current version of Fingerprint image data standard has been tailored from the ISO 19794-4:2005(E) standard to meet specific needs of e-Governance applications in Indian context. It also includes best practices recommended for implementation of the specifications in different categories of e-Governance applications.

The standard is quite extensive to cover the requirements of all categories of civilian e-Governance applications. The applications may judiciously select the specifications relevant to their needs.

1.1 Scope

Usually, the fingerprint image data captured during enrolment is stored / transmitted for 1:1(verification) and 1: N (identification) in an e-Governance application life cycle.

The matching of the fingerprints is done by extracting the minutiae of fingerprint data already stored in the enrolment stage, with the minutiae of data captured at the time of verification/ identification. This process may even require transmission of fingerprint image data / minutiae data among various e-Governance applications by following the best practices.

This standard specifies fingerprint image specifications in different stages like acquisition for enrolment / verification / identification, storage and transmission. It also includes minutiae template specifications and best practices for implementation of the standard specifications in different categories of e-Governance applications based upon the volume of data, and verification/ accuracy requirements.

The current version of the standard is applicable to **all civilian e-governance applications** as the present version does not include specifications for latent fingerprint data required by certain law enforcement applications.

This version of standard addresses the standard specifications for the process of verification using minutiae data. Pattern features and skin pore features are not addressed in this version of the standard.

This standard is structured as follows:

Sections 1 to 4 cover scope, objectives, a brief description, target audience, type of enforcement category, definitions & acronyms etc. The standard specifications are mentioned in section 5. Section 6 includes recommended best practices for various categories of e-Governance applications.

1.2 Objective/Purpose

The e-Government applications deal with Fingerprint data at different stages as follows:

- a. Image acquisition and its storage in the enrolment stage
- b. Image acquisition and storage for offline/ online verification of fingerprint data in 1:1 matching stage
- c. Image acquisition and storage for the purpose of identification in 1:N matching stage
- d. Transmission of finger image data to/from limited memory devices or to/from from image capture device and central verification server or for data exchange with other e-Governance applications
- e. Extraction of minutiae from fingerprint images (during the enrolment or identification/verification stage), their storage, and minutiae matching.

It is possible that different fingerprint capturing devices and software (compression algorithms and matching algorithms) are used at different stages as mentioned above. The purpose of this standards document is to standardize the specifications for fingerprint devices, fingerprint image, storage/transmission and minutiae specifications to ensure interoperability among various fingerprint sensors and algorithms by which the fingerprint images are captured/ stored.

1.3 Applicability

These biometric Standards would be applicable to all e-Governance applications in India as per the Government's Policy on Open Standards.

1.4 Description

A fingerprint is an impression of the friction ridges found on the inner surface of a finger or a thumb. The ridges follow a global pattern identified as whorl, right loop, left loop, arch, tented arch and twin loop etc. Skin pores also present a detailed pattern in fingerprints. There are also local patterns where ridges end or bifurcate, known as **minutiae**.

Local and/or global patterns of fingerprints are matched to provide a means of identification or verification. The science of fingerprint recognition constitutes accurate means of positive identification known to humans.

2. Target Audience

All E-Governance projects of the central and state Government or any other organization that need to comply with this standard for the purpose of interoperability

Vendors of fingerprint devices or software developers for conversion of images to different standard formats, quality evaluation software, minutiae extraction and matching algorithms etc.

All integrators/service providers for Indian e-Governance applications.

3. Type of Standard Document

Type

Standard Specification and Best Practices

Enforcement Category

Standard Specifications: Mandatory

Best practices: Recommended

4. Definitions and Acronyms

Refer Annexure – I

5. Specification of Fingerprint Image Standard

Indian e-Governance Standard will adopt ISO-19794-4:2005(E) Fingerprint Image Data Standard as Indian Standard. (Latest amendments/enhancements issued by ISO to this standard are being examined for adoption in future versions)

To ensure interoperability among vendors, it is required that these images be stored in a format compliant with the international standard ISO 19794-4, within the overall Common Biometric Exchange Formats Framework (CBEFF) as per ISO 19785-1.

For this version of the Standard the prescriptive values, exceptions, deviations and additions, if any to the ISO-19794-4:2005(E) are listed in the six sections as follows:

- a. Device Specifications & Setting
- b. Image Specifications
- c. Quality Specifications
- d. Storage Specifications
- e. Minutiae Specifications
- f. Fingerprint Record Format Specifications.

5.1 Device Specifications & Setting

For the purpose of acquisition of fingerprint image data, at the time of enrolment, verification or identification, fingerprint scanning devices need to be used. There is a need to standardize device specifications to ensure interoperability of fingerprint images of the same person, taken at different stages by different scanning devices.

Device specifications cover scanning resolution, pixel depth and dynamic range. A higher resolution device does not necessarily produce better images¹. The biometric samples captured during enrolment need to be the best samples possible.

5.1.1 Enrolment and Identification

The acquisition setting level detailed below can be **31** or **41** in Table 1 of ISO 19794-4

Setting level	Scan resolution (dpcm)	Scan resolution (dpi)	Pixel depth (bits)	Dynamic range (grey levels)
31	197	500	8	200
41	394	1000	8	200

Pixel depth can range between 8 bits and 16 bits.

Refer best practices section 6.1.1 for device certification requirements.

5.1.2 Verification

The acquisition setting level can be **30** and **above** in Table 1 of ISO 19794-4: 2005(E)

Setting level	Scan resolution (dpcm)	Scan resolution (dpi)	Pixel depth (bits)	Dynamic range (grey levels)
30	197	500	8	80
31	197	500	8	200
40	394	1000	8	120
41	394	1000	8	200

Pixel depth can range between 8 bits and 16 bits.

Refer best practices section 6.1.1 for device certification requirements.

¹ 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 197 dpcm (500 dpi) device from one vendor performs better than a 394 dpcm (1000 dpi) device of another vendor. Nevertheless, these attributes are the only transparent way to specify the minimum device requirements for now.

5.2 Image Specifications

5.2.1 Impression Type

5.2.1.1 Enrolment / Identification

Allowed for Enrolment and Identification: 0 (Live-Scan Plain), 1 (Live-Scan Rolled), 2 (Non Live-Scan Plain), 3 (Non Live-Scan Rolled) or 9 (Live-Scan Contactless).

5.2.1.2 Verification

Allowed Impression type codes for verification are: 0 (Live-Scan Plain), 1 (Live-Scan Rolled), 2 (Non Live-Scan Plain), 3 (Non Live-Scan Rolled), 8 (Swipe) or 9 (Live-Scan Contactless).

Refer Table 7 in section 8.3.7 of ISO 19794-4:2005(E) for the different impression type codes.

Refer section 6.1.2 , for best practices

5.2.2 Finger Position

5.2.2.1 Enrolment / Identification/Verification

The valid values for finger position are 0 through 10, 13, 14, 15

- 0 - Unknown Finger
- 1 - 5 Right thumb through right four fingers
- 6 -10 Left thumb through left four fingers
- 13- Plain right four fingers
- 14- Plain left four fingers
- 15- Plain both thumbs.

Refer Table 5 of ISO 19794-4 for other details like maximum finger image area, width and length corresponding to a finger position.

For best practices, *refer section 6.1.2*

5.2.3 Rotation Angle

No rotation angle is permitted during image acquisition for enrolment / identification / verification

For best practices, refer section 6.1.2

5.2.4 Number of Fingers

In general, every additional finger increases accuracy and improves the possibility of better matching. However, in view of constraints of storage space, the number of fingers to be captured should be optimized depending upon the purpose, sensitivity and accuracy requirements of the e-Governance applications.

5.2.4.1 Enrolment/ Identification

A maximum number of **10** fingers can be captured and minimum number can be **1** finger.

5.2.4.2 Verification

Minimum number of **1** finger is to be captured.

5.2.5 Fingerprint Acquisition Format

5.2.5.1 Enrolment

Lossless (RAW, PNG or Lossless JPEG2000²) image format (compression algorithm code numbers 0, 1, 4, 5 of ISO 19794-4:2005(E)).

5.2.5.2 Verification

In addition to above formats, JPEG2000 with compression ratio up to 1:15 (compression algorithm code Number 2 of ISO 19794-4:2005(E)) is also allowed.

For best practices, refer section 6.1.2.

5.3 Quality Specifications

Captured image must be checked for image quality before storage/minutiae extraction. While many proprietary algorithms claim their superiority as image quality indicators, NIST Fingerprint Image Quality (NFIQ) is publicly available and has been widely used. Hence the same is adopted by this standard also.

Images captured with **NFIQ value of 1, 2 and 3 qualify for acceptable quality.**

NFIQ levels 4 and 5 are poor quality images for minutiae data creation and are discouraged from use for enrolment/verification/identification purposes. However, if it is not possible to obtain desired quality images even after **four attempts**, the best one out of these attempts may be accepted for storage/matching.

For best practices refer section 6.1.3.

5.4 Fingerprint Storage / Archival and Transmission Specifications

Once the fingerprint image gets qualified, it needs to be stored / transmitted for future reference/minutiae extraction.

5.4.1 Storage / Archival Specifications

The fingerprint image would be stored in Fingerprint Image Format, which includes Header details, and image data details (*Refer section 5.6* for detailing).

5.4.1.1 Storage / Archival Format for Normal Memory Devices

PNG (compression algorithm code no 5 of ISO 19794-4:2005(E))

The example of such device is Desk top client / Server.

Note: The image stored for enrolment purpose should never undergo lossy compression at any stage from the instant of capture to storage in database.

² The usage of term JPEG2000 in this document means JPEG2000 part- 1 (for static/still image), or JPEG-2000 Basic or JPEG-2000 Core Coding System, or ISO/IEC-15444-1

5.4.1.2 Storage Format for Restricted Memory Devices

JPEG2000 with compression ratio up to 1:15 (compression algorithm code no 2 of ISO 19794-4:2005(E))

The examples of such devices are Smart card, mobile phones etc.

5.4.2 Transmission Format for Verification

5.4.2.1 Normal Bandwidth

PNG

5.4.2.2 Restricted Bandwidth

JPEG2000 with compression ratio up to 1:15

5.4.3 Transmission Format for Storage

5.4.3.1 For Normal Memory Devices

The fingerprint image captured during the enrolment process should be transmitted in lossless format (*RAW, PNG or Lossless JPEG2000*) from client system to the server for storage / archival in the standardized format for future usage.

5.4.3.2 For Restricted Memory Devices

The fingerprint image can be transmitted in JPEG2000 format with compression ratio up to 1:15.

5.5 Minutiae Data Format Specifications

ISO/IEC 19794-2:2005(E) Finger Minutiae data standard would be adopted in this version of the standard. The mandatory values in this format specified in the ISO 19794-2:2005(E) standard should be used for the purpose of matching.

While the extended data area allows for the inclusion of proprietary data within the minutiae format, this is not intended 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.

To ensure interoperability, there should be a version of the minutiae matching algorithm that does not utilize the proprietary information.

For best practices refer section 6.1.5.

5.6 Fingerprint Image Record Format

This is a format to store biometric data within a biometric data record to cater to interoperability requirements of the biometric data taken by various image acquisition devices. This format also stores specific information related to the fingerprint images.

CBEFF (Common Biometric Exchange Formats Framework) described in ISO 19794-4 will be adopted. This format is based on ISO 19785-1.

As per ISO 19785-1, ISO 19794-4 and ISO19794-5, the Common Biometric Exchange Format Framework (CBEFF) is structured as follows:

- **SBH (Standard Biometric Header)**
- **BDB (Biometric Data Block) for Fingerprint**
 - General Record Header Image Record Header
 - Image Data Block
- **Image Data (Compressed/Uncompressed)**

CBEFF Signature (This is optional as it is used for encrypting and digitally signing the data, wherever required)

Refer section 6.3 for detailing of Finger image record format.

6. Best Practices

The e-governance standards are intended for a variety of applications with varying degree of sensitivity and volume requirements. The specifications in section 5 are broad in nature to cater to all types of e-Governance applications. This section covers the best practices suitable for various categories of applications.

6.1 Best Practices for Implementation of Fingerprint image Specifications

6.1.1 Device Specifications

During enrolment / identification stage, application may appropriately decide about the requirement of certification of fingerprint scanner device by nationally / internationally accredited certification body.

Only those devices to be used, which meet the fingerprint image specifications.

6.1.2 Image Specifications

Refer section 5.2.1 for **Impression Type Specifications**

Although live scan and non live scan images meeting the standard specifications do not have interoperability issues, but matching a non live scan image with a live scan image, may not give the same accuracy as matching two live scan images. Hence the impression types, 0 and 1 should be preferred in e-Governance applications for enrolment, identification and verification.

In case of legacy applications for specific local requirements, impression types 2/3 can also be allowed for operational requirements.

However, in the new versions of the legacy application, it is advised to collect Fingerprint image data from live-scan devices (impression types 0/ 1/ 9) only.

Refer section 5.2.2 for **Finger position specifications**

The choice of finger position would be application dependent, and there should be clear directions indicating which finger (s) data are to be captured for enrolment/ verification/ identification.

In case of enrolment, while using 13, 14 or 15 (4+4+2), the original image should be stored along with coordinates of each finger or segmentation and storage of each finger separately, depending upon the applications requirements.

Refer section 5.2.3 for **Rotation Angle specifications**

Operational Instruction

It is expected that there is no rotation in the finger. Supervised capturing is recommended to ensure that there is no rotation or the device must ensure automatic rotation correction.

	Specifically for enrolment and identification, the vendor needs to ensure minimal rotation (not necessarily "0" angle) with the help of rotation detection and correction algorithm.
<i>Refer section 5.2.4 for</i> No. of Fingers specifications	<p>For Enrolment / Identification The number of fingers to be captured should be based on the</p> <ul style="list-style-type: none"> (a) Total population of the enrolment (b) interoperability needs (c) de-duplication plans. <p>For any state wide or larger enrolment, ten fingers should be captured for de-duplication. A smaller enrolment for access control or district level benefit scheme could use less number of fingers. If there are no plans to perform de-duplication or identification, one or two fingers may suffice.</p> <p>If capturing 1 or 2 fingers, the index finger(s) should be captured. If capturing 4 fingers, two index fingers and two thumbs should be captured.</p> <p>Any finger option Number of fingers to be enrolled will be application dependent. However, for national database of person identification, capturing of 10 fingers data is recommended. For operational ease, in case of 10 finger enrolment, 4+4+2 slab could be considered. The option of capturing by other devices also is open.</p> <p>There should be clear operational instructions to ensure that the correct finger positions are linked with the stored images</p> <p>For Verification Normally only 1 finger is required. In situations requiring higher level of accuracy, two or more fingers may be used.</p>
<i>Refer section 5.2.5 for</i> image acquisition specifications	<p>As per applications requirements, the fingerprint images need to be captured with the devices, which meet the fingerprint image specifications, and image capturing format as specified in section 5.2.5</p> <p>Process of Image Acquisition Refer section 6.2 for best practices for process of image acquisition for enrolment, identification, verification.</p>
<i>Refer section 5.2.5.2 for specifications for</i> fingerprint acquisition for verification in less demanding applications	In case of e-Governance applications requiring fingerprint image verification from local data base only, and the accuracy/sensitivity level is not very high then the image acquisition can be even in JPEG2000 with compression up to 1:15.

6.1.3 Image Quality Specifications

*Refer section 5.3 for
Finger Image Quality
specifications*

The capture software should have an automatic mechanism to check the NFIQ level of captured image, on the spot. The software should accept images with NFIQ quality levels 1/2/3 only, or accept best out of five attempts, in case the image of a person does not fall within acceptable NFIQ level.

You may get poor quality image under circumstances like:

- a) Due to environmental conditions
- b) Due to the ridges being worn out
- c) Due to injury to the finger(s)

In case of (b) and (c), best quality fingerprint image out of 5 attempts may be considered.

In case of 'a' following operational instructions may be followed:

- i. Operator to guide enrollee hand and apply pressure if necessary to obtain best possible image quality.
- ii. For corrective measures and re-tries, operator to wipe the finger(s) of enrollee with wet cloth or apply lotion.

Note: The operators need to be trained on the above

6.1.4 Minutiae Data

*Refer section 5.5 for
minutiae data
specifications*

Every minutiae matching algorithm must have a version that utilizes at least the mandatory standard values in the minutiae storage format for matching. This ensures that each algorithm has at least one version that is completely interoperable.

The matcher and extractor algorithm should have participated and should be listed in the MINEX interoperability test or any other equivalent test.

6.2 Best Practices for Various Processes

6.2.1 Enrolment Process

I. Process at Client end

- a. Capture fingerprint Image data through a fingerprint image scanner connected with a computer for on-line processing, as per the standard specifications
- b. Do Segmentation of the image for quality check
- c. Do quality check of captured image online as per the standard specifications
- d. Store un-segmented image with segmentation coordinates data in secure manner on Client machine in the format, as per standard specifications, along with demographic data of the enrollee, if available.

- e. Transmit the image to the server, in its native captured format or lossless compressed format, as per the standard specifications.

II. Process at Server end

- a. Create biometric template to be used for identification or de-duplication
- b. Compare enrollee's biometric data against entire database (1: N identification) stored on the server to ensure that enrollee is not being enrolled second time
- c. Depending upon the type of e-Gov. Application, decide either to reject the biometric data of enrollee or identify the subject accurately
- d. Store/Archive the Biometric data(un-segmented image with segmentation coordinates data) of the enrollee in format as per standard specifications, on the server database, in case the data was not found on the server earlier.

6.2.2 Verification Process

- a. **Capture fingerprint image data** through a fingerprint image Scanner connected with a computer for **online verification**, as per the standard specifications.
- b. Do segmentation of image for quality check
- c. **Do quality check online** as per the standard specifications
- d. Extract features and **Create minutiae data template**
- e. For **on-line verification**, do 1:1 matching of captured biometric data with the corresponding data from the server.
- f. For **off-line verification**, do 1:1 matching of minutiae of captured image data with the minutiae of corresponding image data stored on the smart card / Client system itself.

6.2.3 Process for capturing rolled fingerprint images

The rolled image, common in forensic applications, contains twice as much information as the plain image. The plain image is easier to capture and the capturing of rolled image of enrollee requires guidance by a trained operator.

6.3 Fingerprint Record Format Specifications

Refer section 5.6 for Fingerprint Record Format specifications

- a. Values in **shaded rows** are variable in nature and need to be entered on case- to **case basis**.
- b. Values in other rows are fixed in nature as per ISO 19794-5:2005(E) specifications and should not to be altered.

Fingerprint Biometric Data Block (BDB) (Extracted from ISO 19794-4)**Table 1 for General Record Header**

Field	Size	Value
Format Identifier	4 bytes	0x46495200 ('F' 'I' 'R') – Finger Image Record
Version Number	4 bytes	0x30313000 ('0' '1' '0' 0x0)
Record Length	6 bytes	General Record Header length+ No. of Views * (Image Record Header Length + Image Data Length) 32+ Number Views * Example: (14 bytes + Data length) 32+1*(14+12028)=12074 bytes
Capture Device ID	2 bytes	0x0 by default
Image Acquisition Level	2 bytes	Value as per section 5.1.1 requirements
Number of fingers	1 byte	Value as per section 5.1.2 requirements
Scale units	1 byte	Value 0x02 representing pixels per cm as per section 8.2.8 of ISO 19794-4:2005(E) Note: Unit ppi not allowed
Scan Resolution	2 bytes	Value as per section 5.1.1 requirements
Scan Resolution (Vert.)	2 bytes	Value as per section 5.1.1 requirements
Image Resolution	2 bytes	Value as per section 5.1.1 requirements
Image Resolution (Vert.)	2 bytes	Value as per section 5.1.1 requirements
Pixel Depth	1 byte	Value as per section 5.1.1 requirements
Image Compression Algorithm	1 byte	Value as per section 5.4 requirements
Reserved	2 bytes	'0x0' – default value

Table 2 for Image Record Header

Field	Size	Values
Length of finger data block (bytes)	4 bytes	To be calculated
Finger position	1 byte	Values as per section 5.2
Count of views	1 byte	Values as per section 5.6 requirement
View number	1byte	"0x1"
Finger image quality	1 byte	Actual value as per section 5.3 requirements
Impression type	1 byte	Values as per section 5.2
Horizontal line length	2 bytes	Value as per input fingerprint image device
Vertical line length	2 bytes	Value as per input fingerprint image device
Reserved	1 byte	'0x0' – default value
Finger image data	< 43x10 ⁸ bytes	Value as per input fingerprint image

7. Annexure

Annexure –I

Definitions and Acronyms

(Source: Various ISO Standards, ICAO Standards, Wikipedia etc.)

Acquisition

Process of accepting a biometric sample(s) in accordance with the defined policy, that is deemed suitable for creating a biometric reference or a biometric probe.

Note: In addition to capture, acquisition may include segmentation, biometrics feature extraction, quality control and other pre-processing steps.

Biometrics

[Automated] recognition of [living] persons based on observation of behavioural and biological (anatomical and physiological) characteristics.

Biometric system

An automated system capable of:

- a. Capturing a biometric sample from an end user;
- b. Extracting biometric data from that sample;
- c. Comparing the biometric data with that contained in one or more reference templates;
- d. Deciding how well they match; and
- e. Indicating whether or not an identification or verification of identity has been achieved.

Biometric data

The data representing biometric characteristic

Example: sensor data, image data, behavioural data, feature data

Note: For the purpose of this document, biometric data refers to fingerprint Image data.

Biometric Data Block (BDB)

Block of data with a defined format that contains one or more biometric samples or biometric templates

Biometric Information Record (BIR)

Data structure containing one or more BDBs together with information identifying the BDB formats, and possibly further information such as whether the BDB is encrypted.

Biometric sample

Data obtained from a biometric device, either directly or after processing.

Biometric Template

Biometric sample or combination of biometric samples that is suitable for storage as a reference for future comparison

Biometric sample

Information obtained from a biometric device, either directly or after processing

Capture

The process of taking a biometric sample from an end user.

Capture device type ID

The capture device type ID shall be a unique identifier for the type of capture device deployed to acquire a biometric sample. The capture device type ID shall be recorded in two bytes. A value of all zeros indicates that the capture device type ID is unreported. The value "unreported" may not be allowable in some applications. The value field is determined by the vendor possibly depending on requirements for the respective application

Friction ridge

The ridges present on the skin of the fingers and toes, the palms and soles of the feet, which makes contact with an incident surface under normal touch. On the fingers, the unique patterns formed by the friction ridges make up fingerprints.

Enrolment

In enrolment, a transaction by a subject is processed by the system in order to generate and store an enrolment template for that individual.

Enrolment typically involves:

- Sample acquisition;
- Segmentation
- Quality checks, (which may reject the sample/features as being unsuitable for creating a template, and require acquisition of further samples);
- Features extraction and template creation (which may require features from multiple samples), possible conversion into a biometric
- Data interchange format and storage;
- Test verification or identification attempts to ensure that the resulting enrolment is usable;
- Should the initial enrolment be deemed unsatisfactory, repeated enrolment attempts may be allowed (dependent on the enrolment policy).

Note: An accept or reject decision is then based on whether this score exceeds the given threshold.

Identification

In identification, a transaction by a subject is processed by the system in order to find an identifier of the subject's enrolment. Identification provides a candidate list of identifiers that may be empty or contain only one identifier. Identification is considered correct when the subject is enrolled, and an identifier for their enrolments in the candidate list. The identification is considered to be erroneous if either an enrolled subject's identifier is not in the resulting candidate list (false-negative identification error), or if a transaction by a non-enrolled subject produces a non-empty candidate list (false-positive identification error).

Identification typically involves:

- Sample acquisition;
- Segmentation and feature extraction;
- Quality checks (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples);
- comparison against some or all templates in the enrolment database, producing a similarity score for each comparison
- Judgment on whether each matched template is a potential candidate identifier for the user, based on whether the similarity score exceeds a threshold and/or is among the highest scores returned, producing a candidate list;
- An identification decision based on the candidate lists from one or more attempts, as dictated by the decision policy.

Intermediate biometric sample

Biometric sample obtained by processing an acquired biometric sample, intended for further processing

Latent

A fingerprint collected from an intermediate surface rather than directly via a live capture from the finger itself.

Live capture

The process of capturing a biometric sample by an interaction between an end user and a biometric system.

Live-scan print

A fingerprint image that is produced by scanning or imaging a live finger to generate an image of the friction ridges.

Matching

The process of comparing biometric data with a previously stored biometric template and scoring the level of similarity.

Note An accept or reject decision is then based on whether this score exceeds the given threshold

Policy

Course or principle of action adopted or proposed by an organization or individual

Resolution

Number of pixels per unit length

Note: Pixels per centimetre (ppcm) will be used in this part of Biometrics Indian e-Governance standard as the unit of resolution.

Standard Biometric Header

Provides encoding for abstract values of CBEFF data elements and enables an application to obtain knowledge about the format and other properties (such as creation date) of the BDBs that are contained in the BIR without having to process the BDBs themselves

Note: *BDBs are not required to be (and generally are not) self-identifying. Identification of BDB formats is provided in CBEFF data elements.*

Swipe

A method of fingerprint collection where the finger is manually moved across a one-dimensional sensor to produce a two-dimensional image.

Verify

Make sure or demonstrate that something is true, accurate or justified.

Verification

In verification, a transaction by a subject is processed by the system in order to verify a positive specific claim about the subject's enrolment (e.g. "I am enrolled as subject X"). Verification will either accept or reject the claim. The verification decision outcome is considered to be erroneous if either a false claim is accepted (false accept) or a true claim is rejected (false reject).

Verification typically involves:

- sample acquisition,
- segmentation
- quality checks (which may reject the sample/features as being unsuitable for comparison, and require acquisition of further samples),
- Features extraction and comparison of the sample features against the template for the claimed identity producing a similarity score,
- Judgement on whether the sample features match the template based on similarity score exceeding a given threshold,
- A verification decision based on the match result of one or more attempts as dictated by the decision policy.

Example In a verification system allowing up to three attempts to be matched to an enrolled template, a false rejection will result with any combination of failures-to-acquire and false non-matches over three attempts. A false acceptance will result if a sample is acquired and falsely matched to the enrolled template for the claimed identity on any of three attempts.

Abbreviated Terms

API	Application Programming Interface
BDB	Biometric Data Block
BIR	Biometric Information Record
CBEFF	Common Biometric Exchange Formats Framework
DPCM	Dots per centimetre
DPI	Dots per inch
PPCM	pixels per centimetre
PPI	pixels per inch
SBH	Standard Biometric Header
SB	Security Block
PNG	Portable Network Graphics
WSQ	Wavelet Scalar Quantization (WSQ), a grey-scale Fingerprint Image Compression Algorithm

8. References

Normative References

- [1] ISO 19794-4 Information Technology – Biometric data interchange formats – Part 4 Finger image data.
- [2] ISO/IEC 19785-1, Information technology – Common biometric exchange formats framework – Part 1: Data element Specification.
- [3] 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
- [4] IAFIS-IC-0110 (V3), WSQ Gray- scale Fingerprint Image Compression Specification 1997
- [5] ANSI/NIST-ITL 1-2000, Information systems – Data Format for the Interchange of Fingerprint, Facial and Scar Mark & Tattoo (SMT) Information
- [6] ISO/IEC 19784-1 Biometric Application Programming interface – Part1: BioAPI specification
- [7] ISO/IEC-15444-1 Information technology – JPEG2000 image coding system : Core coding system
- [8] NISTIR 7151 August 2004 Fingerprint Image Quality.

Other References

- [1] Biometric Design Standards for UID Applications version 1.0, December 2009
- [2] Comparative performance analysis of JPEG2000 vs. WSQ for fingerprint image compression by Nalini K. Ratha, Ruudm.Bolle
- [3] Expert Committee for Mapping Open Standards Principles to Technology Standard of Interoperability Framework for e-Governance(IFEG) for referred image storage formats like uncompressed lossless (uncompressed , PNG) and JPEG2000 for static image
- [4] Government of India's Policy on Open Standards for e-Governance

9. List of Contributors

Expert Committee Contributors

S. No	Name & Designation	Email Address
1.	Professor Manindra Agrawal (Chairman) Department of computer Science & Engineering Indian Institute of Technology (IIT), Kanpur.	manindra@cse.iitk.ac.in 9935062605
2.	Mr. S. K. Sinha (Nodal Officer) Scientist F , NIC, New Delhi	sinha.sk@nic.in
3.	Dr. Mayank Vatsa Assistant Professor, IIIT Delhi	mayank@iiitd.ac.in
4.	Dr. Richa Singh Assistant Professor, IIIT Delhi	rsingh@iiitd.ac.in
5.	Shri G.S. Raghu Raman CMC Limited , Hyderabad	raghuramam.gadepally@cmcltd.com
6.	Mr. R. Ramesh Scientist E , OTC, NIC, Chennai	rramesh@nic.in

Technical Expert on Biometrics

S. No	Name & Designation	Email Address
1.	Dr. Krithika Venkataramani Asst. Professor , IIT Kanpur	krithika@cse.iitk.ac.in
2	Mr. Rajesh Mashruwala Member, UIDAI	mashru@iitbombay.org

Other Contributors

S. No	Name & Designation	Email Address
1.	Mrs. Aruna Chaba Scientist F & Head, e-Governance Standards Division, NIC, New Delhi	chaba@nic.in
2.	Dr. P. Balasubramanian Scientist G & Head OTC, NIC, Chennai	p.balu@nic.in
3.	Ms. Renu Budhiraja, Director (Egov Division), DIT , New Delhi	renu@mit.gov.in
4.	Ms. Anita Mittal Senior Consultant , DIT, New Delhi	am4anitamittal@gmail.com
5.	Dr. Meenakshi Mahajan Scientist E, NIC, New Delhi	meenakshi.mahajan@nic.in
6.	Mr. Rajnish Kumar Sharma Junior Research Fellow, NIC, New Delhi	rajneesh.sharma@nic.in