

**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	
<i>Refer section 5.3 for Finger Image Quality specifications</i>	<p>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.</p> <p>You may get poor quality image under circumstances like:</p> <ol style="list-style-type: none"> a) Due to environmental conditions b) Due to the ridges being worn out c) Due to injury to the finger(s) <p>In case of (b) and (c), best quality fingerprint image out of 5 attempts may be considered.</p> <p>In case of 'a' following operational instructions may be followed:</p> <ol style="list-style-type: none"> 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. <p>Note: The operators need to be trained on the above</p>
6.1.4 Minutiae Data	
<i>Refer section 5.5 for minutiae data specifications</i>	<p>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.</p> <p>The matcher and extractor algorithm should have participated and should be listed in the MINEX interoperability test or any other equivalent test.</p>

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, Ruudnm.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