Face Liveness Detection

ID : SU-C1-2025-01

1. Overview

Currently, during enrolment, a human operator captures images of the subject via a webcam connected to an enrolment client application. The images comply with ICAO passport standards, but the process remains vulnerable to spoofing attempts. Similarly, during authentication, UIDAI relies on active liveness detection (e.g., blink prompts) that introduces user friction, increases drop-offs, and is still vulnerable to sophisticated spoofing tailored to the prompts.

Presentation attacks (a.k.a. spoofing with use of photos, videos, masks, deepfakes, morphs) deceive verification systems, pose a critical threat to the integrity of Aadhaar enrolment and authentication. To safeguard Aadhaar's ecosystem, UIDAI requires a comprehensive liveness detection framework combining active and passive methods. Such a solution should reliably detect spoofing both at the time of enrolment and during authentication, across India-representative demographics, device classes, and operational environments.

2. Objectives

I. **(Changed: Combined both active and passive problem statements)**

To design and evaluate liveness detection models ,whether passive, active, or hybrid , that minimize user interaction and friction during both enrolment and authentication, thereby improving user experience and reducing drop-offs in Aadhaar face authentication.

II. **SDK**- To develop a SDK that can be integrated into UIDAI's enrolment and authentication applications and frameworks, ensuring compatibility across edge devices and smartphones.

III. **Compliance** - To deliver robust AI/ML solutions capable of detecting both physical attacks

(print, replay, masks, morphs) and digital attacks (deepfakes, adversarial manipulations), while maintaining compliance with UIDAI's privacy and security rules.

3. Challenge Description

Participants are expected to develop active and passive face-liveness detection SDKs that:

a) Detect a wide spectrum of physical and digital presentation attacks, including photos, replayed videos, 2D/3D masks, morphs, deepfakes, and adversarial perturbations.

b) Work seamlessly in both contexts:

- Enrolment: Software solution integrated with UIDAI's Applications and Frameworks, performing liveness detection at the time of face capture.
- Authentication: Software solution / SDK integrated with mobile or handheld devices, ensuring a frictionless, secure user experience.

c) Operate reliably across UIDAI's device classes (PCs for enrolment, smartphones for authentication), varied lighting, environments, and India's demographic diversity.

d) Support edge deployment (low memory footprint on Intel/AMD CPUs for enrolment, lightweight inference on mobile for authentication), as well as server-assisted deployments when feasible.

e) Include configurable active engagement prompts (when needed) while prioritizing passive liveness methods to minimize friction.

4. Solution Design Considerations

a) **Capture**

i. Primary input: short unprompted video clip (1–5s), with support for single-image fallback.

ii. Support for multiple camera classes (webcams used in enrolment, smartphone RGB cameras used in authentication).

b) **Model & Techniques (non-exhaustive)**

i. AI ML Models for motion and consistency cues.

ii. Intuitive designs for passive liveness cue.

iii. Robustness techniques against deepfakes, morphs, and adversarial attacks.

iv. Lightweight edge models for enrolment clients (Intel/AMD CPUs, low memory footprint).

v. Mobile-optimized models for authentication clients (ARM CPUs, limited compute).

vi. Higher-capacity server models for centralized scoring, when available.

c) **Performance & Operational Targets (proposal to justify actual numbers)**

i. Latency: Real-time or near-real-time performance (e.g., ≤1.5s for enrolment, ≤1s for authentication).

ii. Graceful degradation: The SDK should provide a score with a defined fallback behaviour when input quality is low, enabling the application to prompt the user for recapture.

iii. Resource footprint: Optimized for memory and compute constraints of enrolment PCs and smartphones / Tablets.

4.1 Key Results

- Software solutions /SDK(s) for integration with UIDAI's enrolment and authentication apps and frameworks.
- Demonstrated detection accuracy across physical and digital attacks in India-representative scenarios.
- Field-tested models validated on UIDAI sandbox datasets, with ISO/IEC 30107-compliant reports.
- Documentation and integration guides for deployment.

5. Evaluation Criteria

a) Detection Effectiveness — Strong performance across spoofing types (photos, replay, masks, morphs, deepfakes, adversarial inputs), including unseen attack types.
b) Robustness — Stable performance across demographics, devices, lighting conditions, and occlusions.
c) Usability Gains — Reduction in authentication drop-offs compared to current active liveness solutions; seamless integration with enrolment capture workflows.
d) Latency — Meets UIDAI-defined performance benchmarks on both enrolment PCs (Intel/AMD x86) and mobile devices, with average inference time of ≤ 1 seconds.
e) Standards Compliance — Evaluation aligned with ISO/IEC 30107 and NIST FRVT PAD frameworks.
f) Datasets & Reproducibility — India-representative datasets used for training/testing, with reproducible results for third-party validation.
g) Integration Readiness & Security — SDKs tested with UIDAI sandbox, with clear integration plan, secure update mechanisms, and adherence to Aadhaar privacy protocols.
h) Model size of ≤ 6 MB (distributable via the WASM framework)
i) The anti-spoofing mechanism shall achieve an APCER ≤ 0.10% and BPCER ≤ 0.10% following the below definitions:

- **APCER (Attack Presentation Classification Error Rate):** Proportion of attack (spoof) presentations incorrectly classified as bona fide.
- **BPCER (Bonafide Presentation Classification Error Rate):** Proportion of bona fide (genuine) presentations incorrectly classified as attack.