YellowSense Technologies

Face Liveness Detection

PRESENTED BY

Dweep Solanki and Binita Mahto

YELLOWSENSE TECHNOLOGIES

Problem Statement & Proposed Pipeline

Face-based biometric systems are vulnerable to presentation attacks
Common attack types:

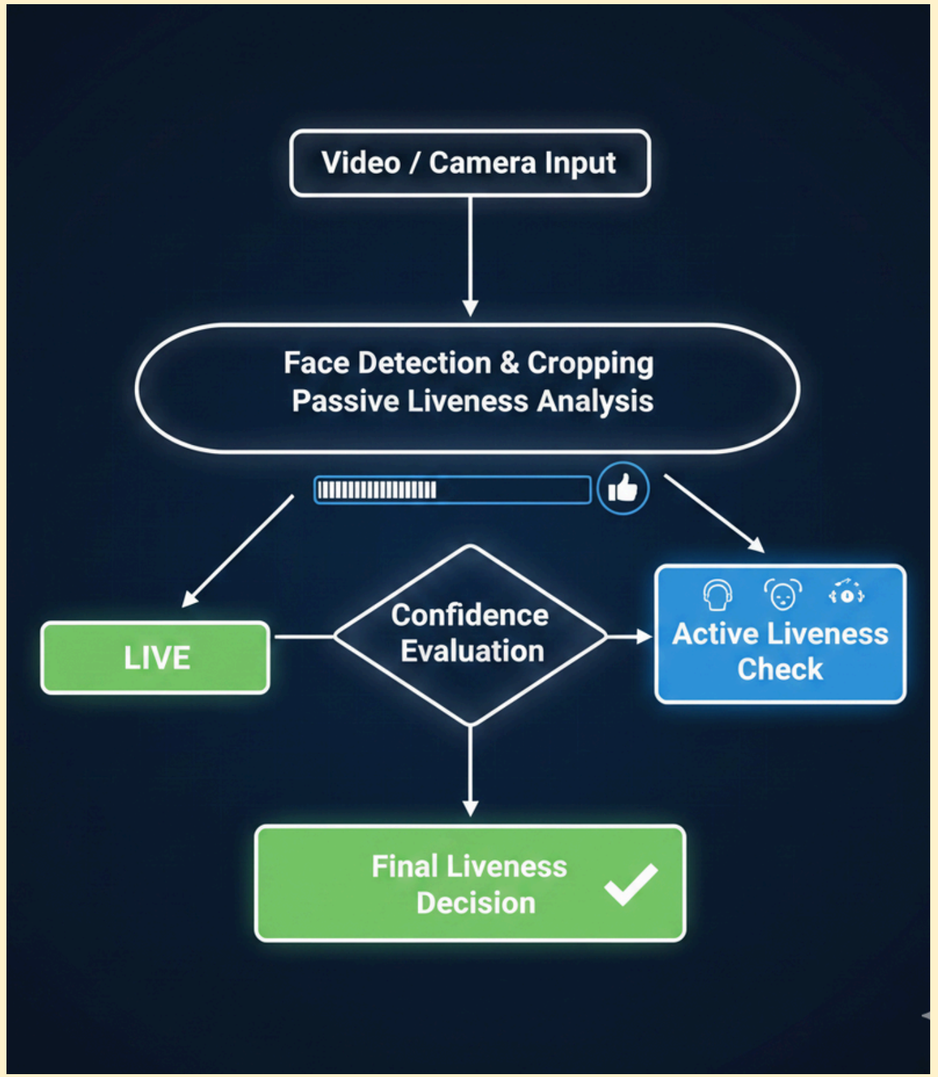
- Printed photographs
- Replayed videos
- Mask-based impersonation
- Synthetic / deepfake media

Existing active-only liveness:

- Increases user friction
- Causes authentication drop-offs
- Can be bypassed by trained attackers

Requirement:

- Low-friction
- High-accuracy
- Real-time
- Edge-compatible liveness detection



YELLOWSENSE TECHNOLOGIES

Solution Overview

Core Idea

- Design a hybrid face liveness detection system
- Combine:

- Passive liveness detection (default)
- Active liveness detection (fallback only)
- Implemented as a backend SDK, independent of UI or platform

How the Solution Works

- System first evaluates passive liveness using:
- Facial motion
- Texture consistency
- Temporal cues from short video
- A confidence score is generated

If confidence is above threshold:

- User is marked LIVE

If confidence is below threshold:

- System triggers active liveness (blink detection)

YELLOWSENSE TECHNOLOGIES

System Architecture

Architecture Overview

- Modular backend design implemented as an SDK
- Clear separation between:
- Data capture
- Liveness analysis
- Decision logic
- Designed for easy integration into enrolment and authentication systems

Core Components

1. Frame Processor
2. Extracts and normalizes video frames
3. Prepares frame sequences for inference
4. Face Detector
5. Detects and crops facial regions
6. Ensures only valid face data is processed
7. Passive Liveness Model
8. Analyzes motion, texture, and temporal features
9. Produces a passive liveness confidence score
10. Active Liveness Detector
11. Performs blink-based verification
12. Triggered only when passive confidence is low
13.
14. Decision Engine (SDK Core)
15. Combines passive and active results
16. Produces final LIVE / SPOOF decision

YELLOWSENSE TECHNOLOGIES

Passive Liveness Detection

What is Passive Liveness?

- Liveness detection without explicit user actions
- Uses natural facial behavior captured from a short video
- No prompts such as blinking or head movement

How Passive Liveness Works

- Input: short unprompted video sequence
- Extracts facial region from each frame

Analyzes:

- Micro-movements
- Texture consistency
- Temporal coherence across frames
- Generates a liveness confidence score between 0 and 1

Model Used

- Lightweight CNN-based model
- Optimized for real-time, CPU-based inference
- Suitable for edge and mobile environments

YELLOWSENSE TECHNOLOGIES

Active Liveness Detection

Passive liveness may be inconclusive in:

- Poor lighting
- Low-quality cameras
- Borderline confidence cases
- Active liveness strengthens the final decision

When Active Liveness is Triggered

- Passive liveness score falls below a predefined threshold
- System automatically switches to active verification
- Ensures security without affecting most genuine users

Active Liveness Technique Used

- Blink detection using eye aspect ratio (EAR)
- Facial landmarks tracked across frames
- Time-bound challenge to prevent replay attacks

YELLOWSENSE TECHNOLOGIES

Hybrid Decision Logic

Decision Strategy

System follows a hybrid liveness strategy
Combines results from:

- Passive liveness detection
- Active liveness detection (if triggered)

Decision Flow

- Passive liveness score is evaluated first

If score ≥ threshold:

- User classified as LIVE

If score < threshold:

- Active liveness challenge is initiated

Final decision is based on:

- Passive score
- Active challenge outcome

YELLOWSENSE TECHNOLOGIES

Backend SDK Design

SDK-Oriented Approach

- Implemented as a backend SDK
- Independent of UI or platform-specific components

Designed for integration into:

- Enrolment applications
- Mobile authentication apps
- Edge-based systems

YELLOWSENSE TECHNOLOGIES

Performance & System Optimization

Performance Goals

- Real-time liveness detection
- Low-latency inference suitable for authentication use-cases
- Smooth execution on consumer-grade devices

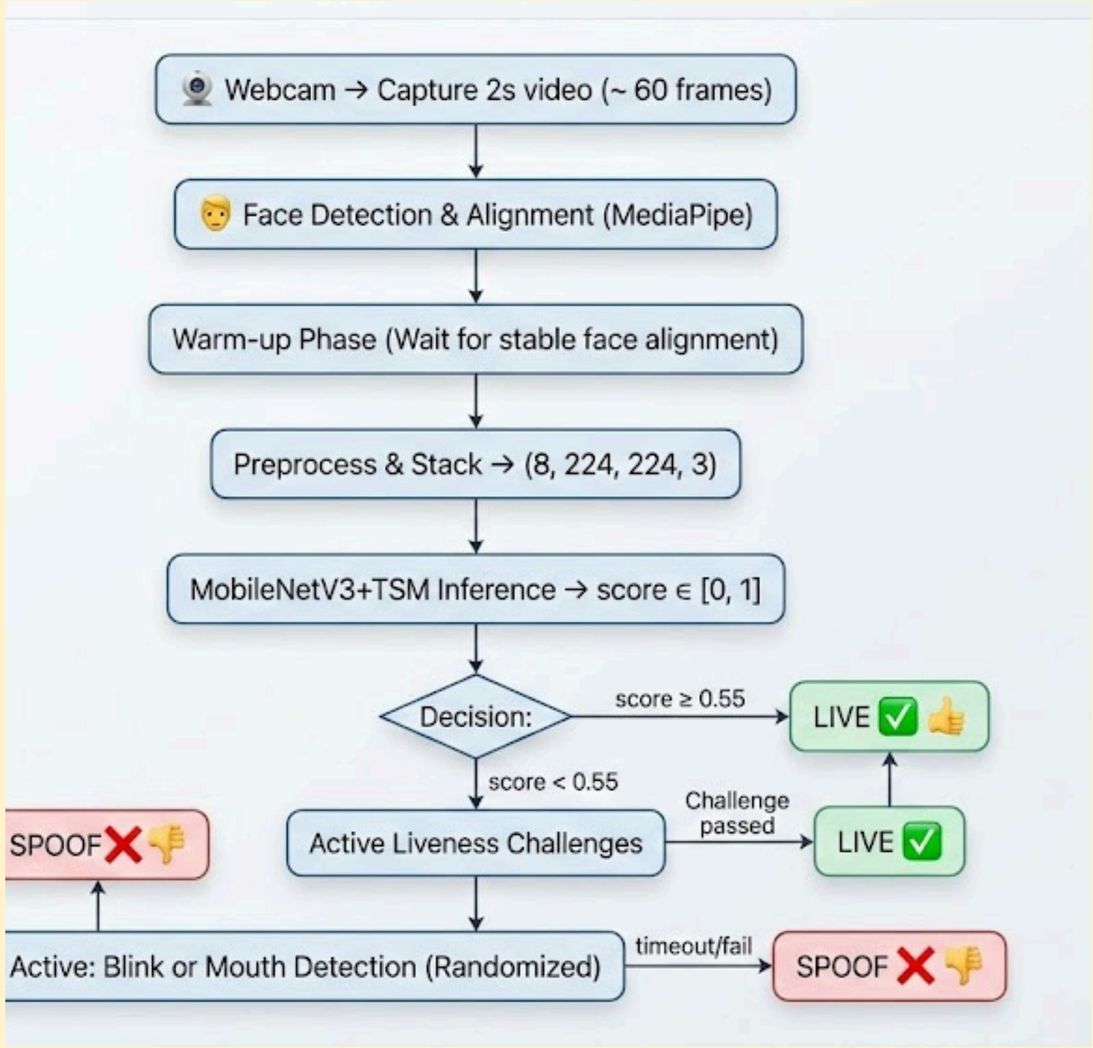
Optimization Strategies

- Lightweight CNN architecture for passive liveness
- CPU-only inference (no GPU dependency)
- Limited frame window to reduce compute load
- Efficient preprocessing and batching of frames

Edge Device Readiness

Designed for:

- Desktop enrolment systems
- Mobile authentication devices
- Minimal memory footprint
- Stable performance across varying lighting and environments



YELLOWSENSE TECHNOLOGIES

Security, Privacy & Compliance

Security Measures

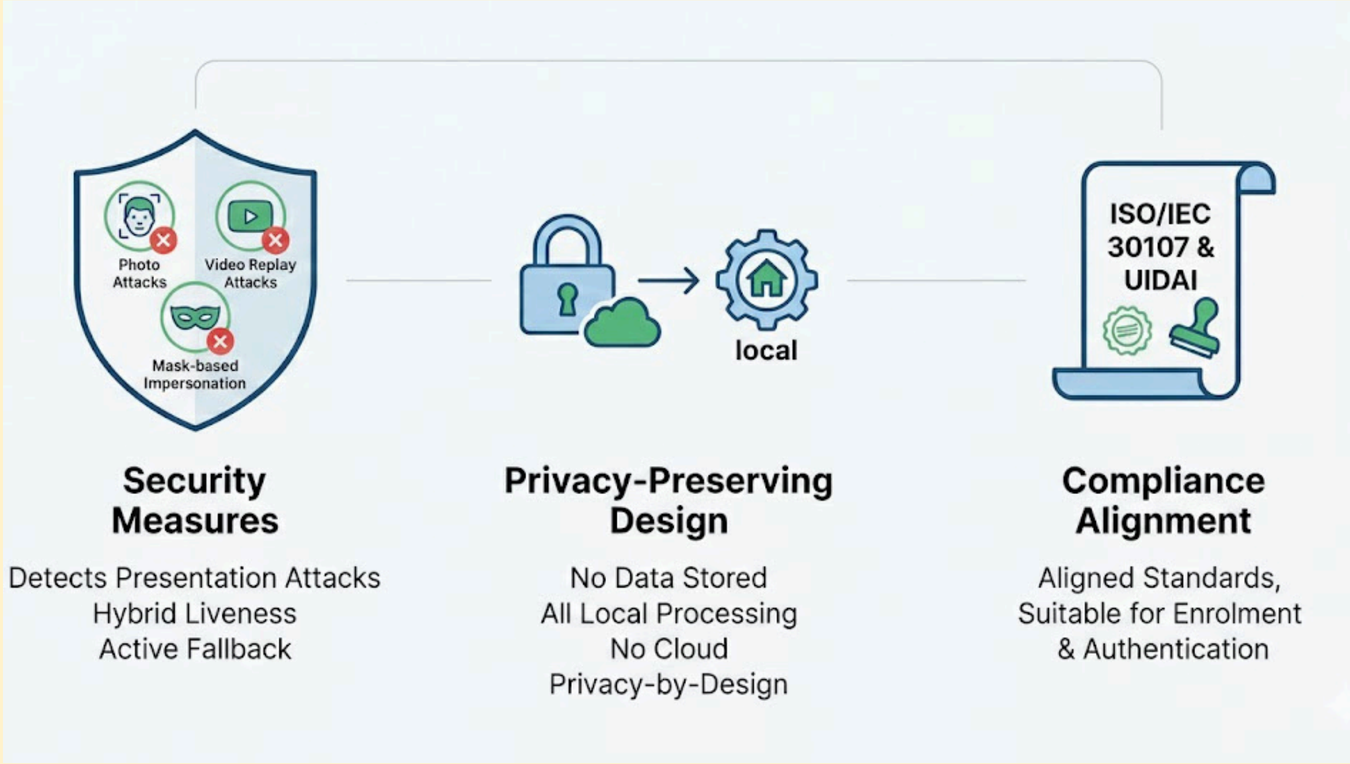
- Detects multiple presentation attacks:
- Photo attacks
- Video replay attacks
- Mask-based impersonation
- Hybrid liveness strategy reduces spoofing success
- Active fallback prevents static and replay-based attacks

Privacy-Preserving Design

- No biometric data stored permanently
- All processing performed locally
- No dependency on external cloud services
- Complies with privacy-by-design principles

Compliance Alignment

- Architecture aligned with ISO/IEC 30107 (PAD) standards
- Designed to meet UIDAI liveness detection requirements
- Suitable for enrolment and authentication workflows



YELLOWSENSE TECHNOLOGIES

Conclusion

This project presents a hybrid face liveness detection backend that combines passive and active verification to effectively defend against spoofing attacks while minimizing user interaction. By prioritizing passive liveness and triggering active checks only when required, the system achieves a balance between security, performance, and user experience. The modular SDK-based design ensures easy integration, real-time execution, and suitability for large-scale biometric authentication systems.