Shufti

Facial Liveness Detection

PCI DSS

SOC2

GDPR

QG GDPR

ISO 27001: 2013

CE+

iBeta Level 1

KJM AGE VERIFICATION

CCPA

With the rise of identity fraud, deepfake attacks, and digital impersonation, businesses need a robust solution to verify users securely and reliably. Traditional authentication methods, such as passwords or document checks, are no longer enough to prevent sophisticated fraud attempts.
Shufti's Facial Liveness Detection ensures that only real, physically present individuals can pass verification by detecting spoofing attempts using AI-driven biometric analysis. It prevents fraudsters from using photos, videos, deepfakes, or 3D masks to manipulate identity verification systems.

What Is Liveness Detection?

Facial Liveness Detection is an AI-powered technology that determines whether a user is a real person physically present during verification. It prevents fraud attempts where attackers use static images, pre-recorded videos, or computer-generated deepfakes to impersonate real individuals.

Shufti utilizes advanced AI-powered techniques for liveness detection, ensuring accurate user verification while preventing spoofing attempts. Below are the key methods used to confirm real user presence and detect fraudulent activity.

Facial Spoofing & Presentation Attack Detection

Fraudsters try to bypass verification using printed images, 3D masks, or video replays. Shufti's presentation attack detection ensures that only real, live users are verified.

- Identifies photo cutouts, digital screen displays, and fake masks
- Uses AI-driven texture analysis to detect unnatural skin surfaces
- Blocks attempt using manipulated images or videos

3D Depth Detection

Shufti performs 3D Depth Detection to ensure that only real, physically present individuals pass verification by analyzing facial depth, contours, and motion patterns. AI-powered depth mapping, light reflection analysis, and motion tracking differentiate real users from spoofing attempts using 2D images, videos, or deepfakes. This technology strengthens fraud prevention across banking, fintech, gaming, and crypto industries.

Skin Texture Analysis

Shufti performs Skin Texture Analysis to enhance the accuracy of face verification and liveness detection by examining fine details such as pores, wrinkles, and skin tone variations. This AI-powered technology differentiates real human skin from artificial surfaces like masks, printed photos, or screen displays, making it highly effective in detecting spoofing attempts and deepfake fraud.

Deepfake & AI-Generated Face Detection

With the rise of deepfake technology, attackers can use AI-generated faces to impersonate users. Shufti's deepfake detection algorithm analyzes skin texture, motion inconsistencies, and visual artifacts to flag fake identities instantly.

- Detects AI-generated faces, morphing attempts, and face swaps
- Prevents account takeovers, digital identity fraud, and synthetic identity creation
- Uses multi-frame analysis to spot inconsistencies in facial features

Duplicate Account Detection

Shufti's Duplicate Account Detection prevents users from creating multiple fraudulent accounts by leveraging facial recognition technology. AI-driven face matching detects repeat registrations, even when users attempt to modify details such as name variations or different identity documents.

Here Is How The Facial Verification Process Works

STEP 01

Enroll

Users select facial biometric authentication, bypassing passwords.

STEP 02

Verify

Users confirm identity with a live selfie and other methods as needed.

STEP 03

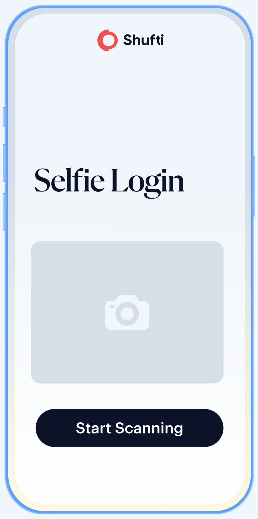
Authenticate

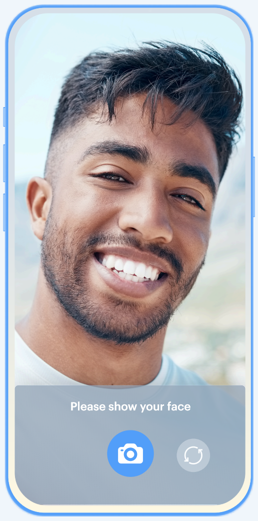
Shufti matches the selfie to stored biometric data.

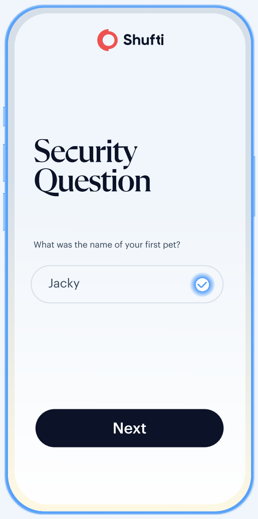
STEP 04

Access

Successful authentication gets users what they need faster.

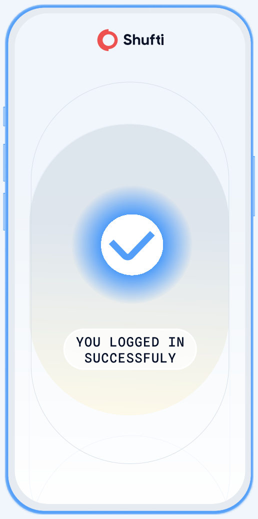






What was the name of your first pet?

Jacky



HOW SHUFTI PERFORMS FACIAL LIVENESS DETECTION

Shufti employs a multi-layered AI approach to verify user presence and detect fraud with high accuracy and minimal friction. Below are the checks performed in liveness detection.

- **Replay Attack / Screen in Screen:** Detects if the image is a replay on a screen to prevent fraud.
- **2D / 3D Mask Detection:** Identifies mask-based impersonation attempts.
- **Paper Mask Detection:** Recognizes faces displayed on paper to simulate a real person.
- **Injection Attacks:** Prevents attempts to bypass the system by feeding it pre-recorded or synthetic facial data instead of live, real-time imagery.
- **Closed Eye Detection:** Ensures that the person has open eyes, confirming alertness.
- **Web Detection:** Detects face images from the internet to prevent digital spoofing.
- **Multiple Faces Detection:** Identifies if more than one face appears in the frame.
- **Screenshot Detection:** Detects if the image is captured from a screen.
- **Solid Background Detection:** Verifies a neutral background for accurate face assessment.
- **Filter Edit:** Identifies if filters that alter the face's authenticity are applied.
- **Face Visibility:** Ensures the face is fully visible for accurate detection.

The need for secure and fraud-proof identity verification spans across multiple industries, where ensuring that users are real and physically present is essential to prevent identity theft, account takeovers, and unauthorized access. Shufti's Facial Liveness Detection helps businesses across industries verify users instantly, securely, and efficiently.

Banking & Fintech

Prevent account takeovers, financial fraud, and unauthorized access by verifying users through biometric authentication. Facial liveness detection ensures that only legitimate account holders can access financial services.

Gaming & Gambling

Online gaming and gambling platforms require strict identity verification to comply with age verification laws and prevent multi-account fraud. Facial Liveness Detection ensures that users are who they claim to be, reducing the risk of fraud and regulatory fines.

Cryptocurrency & Blockchain

The crypto industry is a major target for money laundering and identity fraud. With liveness detection, crypto exchanges can ensure real user authentication, reducing fake account creation and unauthorized withdrawals.

E-commerce & Digital Marketplaces

Prevent fraudulent transactions, chargeback scams, and fake account creation by verifying real users before they make purchases or access sensitive account features.

Healthcare & Telemedicine

Ensure patient identity verification for online consultations, secure medical record access, and prevent insurance fraud using AI-driven facial liveness detection.

Government & Public Services

Governments use biometric verification to secure digital identities, border control, and social services. Liveness detection prevents fraudsters from exploiting government programs or identity-based benefits.

With Shufti's Facial Liveness Detection, businesses across industries can enhance security, compliance, and user trust while preventing fraud in real-time.