Shufti

Truth in identity

The Leading Technological Powerhouse in Identity Verification

PCI DSS

SOC2

GDPR

QG GDPR

ISO 27001: 2013

CE+

iBeta Level 1

KJM AGE VERIFICATION

CCPA

INTRODUCTION

In today's expansive global tech market, where every third individual holds a presence in the global online community conducting business operations and financial transactions. Biometric systems have become an integral part of ensuring the authenticity of an individual in our day-to-day lives. While fingerprint-based biometrics have seen widespread usage, the most rapidly growing biometric identification has been facial recognition. Safety is not security. The IoT needs Safety. Safety is something we as users should control. The IoT has to be user-centric to be the powerful tool it is bound to be, it should never become the door of a prison, which it could potentially become if we allow facial recognition to enter every facet of our lives.

This document provides an in-depth overview of Shufti's advanced verification checks during document and face verification processes. It highlights the range of sophisticated measures employed to ensure the authenticity of identity documents and the liveness of individuals during verification. This document also includes accuracy statistics for these checks, reflecting Shufti’s commitment to providing reliable and secure identity verification solutions.

Facial Biometrics

Shufti’s Facial Biometric Verification leverages AI-driven facial recognition, liveness detection, and deepfake prevention to offer a seamless, secure, and frictionless identity verification experience. As digital fraud tactics evolve, businesses require advanced security measures to verify users with speed and accuracy. By analyzing facial features, skin texture, and depth variations, Shufti ensures that only genuine, physically present users pass verification, preventing spoofing attempts using photos, videos, or AI-generated deepfakes.

Face Verification Process

Shufti performs the following checks to ensure secure and reliable face verification.

Liveness Detection

Ensuring the user is physically present is critical to preventing fraud. Shufti's liveness detection technology analyzes natural movements, blinking, and depth cues to distinguish real users from fake attempts.

- Identifies printed photos, video replays, and digital spoofs.
- Uses blinking, head movements, and light reflection to confirm liveness.
- Prevents bot-driven attacks and impersonation fraud.

Active & Passive Liveness Detection

Shufti offers Active and Passive Liveness Detection to prevent spoofing attacks and identity fraud by ensuring that only real, physically present users pass verification.

- Active Liveness Detection confirms physical presence by requiring real-time interaction, making it impossible for fraudsters to use static images, pre-recorded videos, or deepfake animations to bypass verification.
- Passive Liveness Detection runs silently in the background, analyzing micro-expressions, skin texture, and depth variations without requiring user interaction. AI-driven light reflection analysis and 3D face mapping detect fake faces, printed photos, and screen-based attacks.

By combining both Active and Passive Liveness Detection, Shufti ensures seamless user experience, enhanced security, and real-time fraud prevention across banking, fintech, crypto, and digital identity verification platform

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.

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.

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

Face Match With Document Image

Face matching verifies the similarity between the face presented and the face on the document, ensuring they belong to the same individual. It enhances identity verification by confirming visual consistency.

- Similarity Score Calculation: Quantifies the match between the presented and document faces.
- Face Landmark Matching: Compares facial features for precise alignment.
- Occlusion Detection: Identifies any face obstructions like a partially covered face.
- Eyewear Detection: Detects any eyewear that could obstruct facial visibility.

Document Verification

Shufti's Document Verification enables fast, secure, and accurate customer onboarding while ensuring robust identity fraud protection. Traditional document processing is time-consuming and prone to errors, making it a challenge for businesses to balance efficiency and security. Manual data entry remains a bottleneck, pushing organizations to adopt automated solutions that can accurately extract, validate, and populate critical information. Shufti's AI-powered document verification streamlines this process, enhancing accuracy, reducing fraud, and improving compliance—especially for industries handling financial, legal, and identity-sensitive documents.

- ✓ Instant ID Verification
- ✓ OCR-Based Data Extraction
- ✓ Hologram & Tampering Detection

UK DRIVING LICENCE
1. HARRISON
2. CHARLOTTE
3. 15.10.1988 LONDON
4a. 04.05.2020 4c. DVLA
4b. 03.05.2030
5. DL985632B
7. Harrisonch
8. 12345 BAKER STREET, LONDON, NW1 5XX
9. A/B

Techniques used to check the authenticity of the Document

Shufti performs the following steps to check the authenticity/originality of the Document.

Document Format

Shufti supports more than 3000 document templates in more than 150 languages from 230+ countries. These documents are checked and compared with different templates to minimize the threats of forgery.

Detect Any Crumpled / Folded Edges

The AI-induced system then checks for any folded edges or wear and tear that might be a hindrance on the way of its authenticity.

Authenticity Of MRZ Codes

The document then checks the authenticity of MRZ codes, found mostly on passports and some on Driver's licenses and ID cards. the code consists of the owner's personal data, (that is extracted by using OCR) and a forgery detection number.

Check For Photoshopped / Tempering / Forgery

AI has induced a number of models and templates that can easily detect any kind of tempering used on the document or photoshopped document. If it detects any of the tempered documents, instantly it declines the document and saves the client from any fraud.

Verify Holograms / Rainbow Prints

Government-issued ID cards have specific holograms or rainbows printed over them. To check its authenticity, Shufti has induced a number of templates within the system which detects any tampering with holograms or rainbow prints.

Guilloche

Guilloche printing is an ornate pattern to prevent cards from being forged. The pattern consists of a series of woven, curved lines in a geometric pattern that can be applied in various colors. Shufti is capable of reading these guilloches to check their authenticity.

Optically Variable Ink (OVI)

OVI also called color-shifting ink is an anti-counterfeiting measure used on many major modern banknotes and government-issued ID cards. The ink displays two distinct colors depending on the angle the bill is viewed at. The ML has the capability to check this OVI to verify the documents' authenticity.

Microprinting / Multi Laser Images

Shufti checks for any kind of microprinting and any kind of multi-laser images on an ID card for the authenticity of the document. This whole process can easily be explained with the help of the following image. It will explain what are the measures we are taking to check the authenticity of any government ID cards.