Shufti

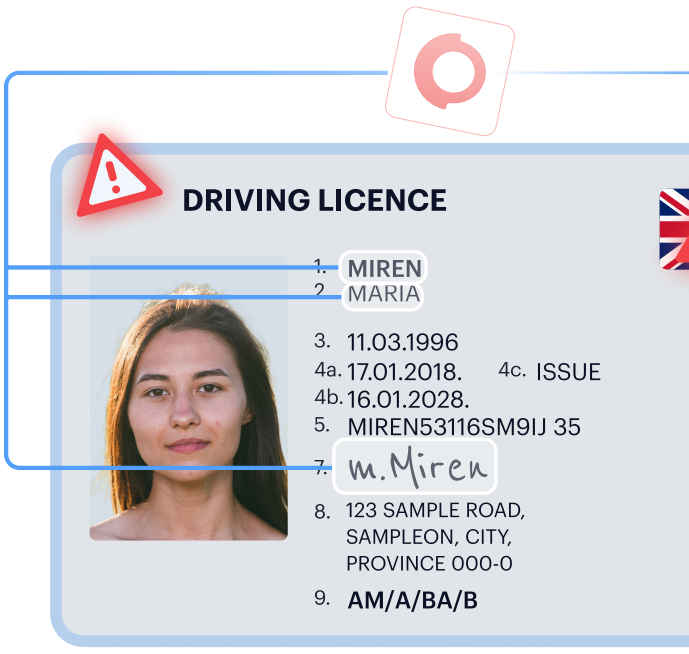
Document Verification

Know Who You're Dealing With. Before It's Too Late.

Document fraud technology is advancing faster than most verification platforms can detect it.

AI tools now produce photorealistic passports, national IDs, and driver's licences that pass basic visual inspection. RGB-only platforms cannot detect them. Manipulation signatures exist in the DCT frequency domain, invisible to visual analysis alone. Global fraud losses hit $27.2 billion in 2024, up 25% in a single year. Every document wrongly accepted is a fraud loss. Every document wrongly rejected is a lost customer.[1]

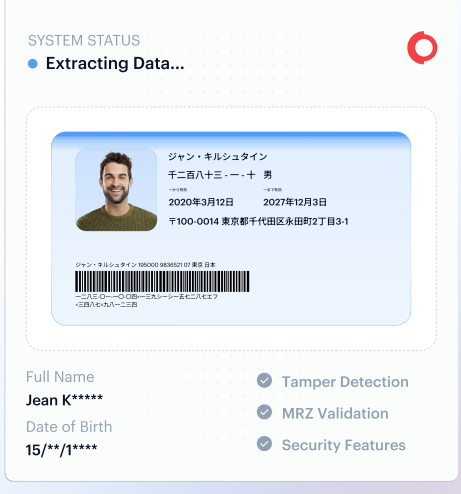
Most vendors check 2–3 layers using template matching and RGB analysis without frequency-domain analysis. Non-Latin OCR fails on Arabic, Vietnamese, and CJK. Sophisticated fraud gets through.



Introducing Shufti's Document Verification

Shufti Document Verification authenticates identity documents in real time using a 9-layer AI-powered forensic pipeline built entirely in-house , no aggregators, no third-party data routing, no ResistantAI dependencies.

Any government-issued document. 250+ countries. 150+ languages. Under 15 seconds. AutoML confidence score. DCT-based deepfake detection. PVC card detection at >95%. One API. Onsite and offsite. Cloud or on-prem.



DHS RIVR 2025 Top Performer

Shufti is one of only five vendors to meet 100% of DHS RIVR 2025 goals, government-validated, not self-reported. The evaluation recorded a false acceptance rate below 0.001%, ~99% true acceptance, sub-3-second verification, and zero failure-to-capture, powered by all nine fraud-detection layers running in-house, including DCT frequency analysis that catches AI-generated documents others miss.

How Shufti's Document Verification Works

Step 01

Document Capture

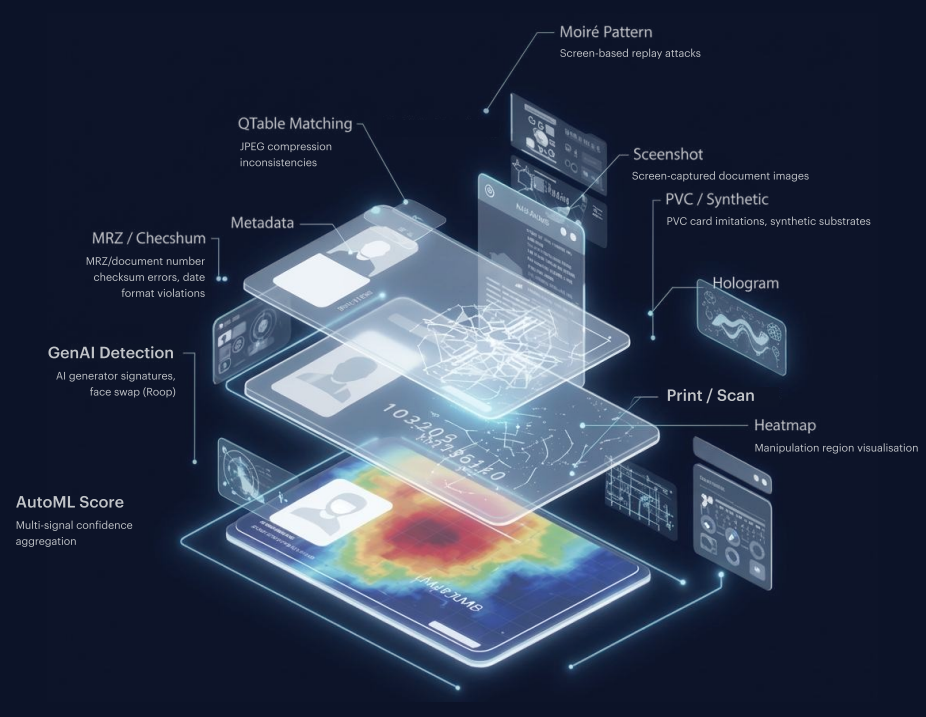
Onsite (SDK + auto-capture): Shufti's intelligence moves to the user's device. Guides users in real time , "Move Closer," "Remove Glare" , and auto-captures only when the image meets quality thresholds. Device fingerprint, session data, and network signals collected at capture. Up to 55% conversion improvement over basic upload.

Onsite (SDK + auto-capture): Server-to-server. Results via webhook callback. No SDK required. For backend integrations and batch processing.

Step 02

9-Layer Forensic Pipeline

Every submission passes through every layer simultaneously. No shortcuts. No third-party dependencies.



Step 03

OCR & Data Extraction

Proprietary in-house OCR at 99.7% accuracy across 150+ languages extracts and validates all critical data fields. Outperforms Google Vision API on every non-Latin script relevant to global onboarding:

Language		
Arabic	92.17%	90.24%
Vietnamese	96.79%	82.36%
CJK (Japanese/Chinese)	86.87%	82.89%
Burmese	94.41%	64.36%

Step 04

Fraud Intelligence

Fraud Memory flags document reuse and re-registration patterns across every submission. PEP and sanctions screening on every decision. Dynamic blacklisting auto-blocks users matching the fraudulent activity database.

Step 05

Decision & Evidence

Confidence score, coded decline reasons, and heatmap artefacts delivered in one exportable audit package , under 15 seconds, stored in a single back office, audit-ready from the first verification.

Why Shufti

The Gaps Your Current Vendor Won't Show You

Most document verification failures are invisible until a regulator finds them. By then the cost is not a chargeback — it is an enforcement action.

Outsourced detection means inherited liability

When a vendor outsources fraud detection, they cannot audit what they do not own. Your compliance team inherits gaps they have no visibility into — and no ability to remediate before an audit.

AI-generated documents have already bypassed most platforms

The forgery methods that concern regulators today operate in the frequency domain. Platforms built on visual signals alone cannot detect what they were never designed to see.

Self-reported accuracy is not a compliance defence

When a regulator or enterprise procurement team asks for independent verification of your vendor's accuracy claims, a vendor-published benchmark is not an answer. Government-validated metrics are.

Physical card fraud passes every vendor that only tests digitally

Manufactured physical documents are designed to pass digital capture. If your vendor does not test physical reproductions, they are not testing for the fraud that is actually in circulation.

Document Verification Feature Matrix

Capability	Details
9-Layer Forensic Pipeline	All nine layers in-house. No third-party dependencies. Competitors check 2–3 layers and outsource the rest.
Deepfake Detection	99% via RGB + DCT frequency analysis. Heatmap evidence on every rejection.
PVC Card Detection	>95% including Japanese PVC , industry first.
OCR Accuracy	99.7% across 150+ languages. Outperforms Google on Arabic, Vietnamese, Burmese, CJK.
Document Coverage	Any government-issued document. 250+ countries. New types added on demand.
Document Two Service	Two documents, one session, one consent capture. Automated cross-check of name, DOB, and document number. Configurable by jurisdiction and risk tier.
Document Intelligence	**Responsible Gambling**, rule-by-rule risk score (Low/ Medium/High) from bank/credit card statements. **Salary Analysis** , income and spending pattern evaluation to detect misrepresentation before credit decisions.
Fraud Memory	Flags document reuse and re-registration patterns across every submission.
Continuous Verification	Document expiry monitoring and automated re-verification triggers across active user base.
Heatmap Visualisation	Pixel-level manipulation evidence on every rejection. Satisfies EU AI Act explainability requirements.
Facial Biometrics (Add-On)	Live face match against document photo. Confidence score 0–100. Liveness detection. 2.98s average. 98.22% acceptance rate.
Deployment	Cloud · On-Prem · Hybrid. PCI DSS. ETSI in progress. SOC 2, ISO 27001.

Key Performance Metrics

0.0163 False Accept Rate	0.0151 False Reject Rate	98.49% True Accept Rate
Zero Failure to Capture	99.7% OCR Accuracy	99% Deepfake Detection
>95% PVC Card Detection	Under 15 Secs Processing Speed	1M+ Verifications/Day Daily Scalability

Regulatory Alignment

GDPR , Articles 5, 22, 30

Relevant Requirement:
Data accuracy and integrity; rationale and contestability of automated decisions; records of processing activities

What Shufti Covers

Metadata integrity validation supports Article 5. Deepfake heatmaps provide field-level forensic evidence for every automated rejection, supporting Article 22 contestability. Logged decisions with exportable audit records support Article 30 record-keeping.

EU AI Act , Article 13

Relevant Requirement:
High-risk AI systems must be sufficiently transparent and accompanied by information/instructions enabling deployers to interpret outputs and use the system appropriately.

What Shufti Covers

Pixel-level heatmap analysis gives compliance teams an interpretable basis for every decision. Downloadable reports with proper reasoning of denying decisions.

FATF Recommendations 10 & 11

Relevant Requirement:
Verify customer identity using reliable, independent source documents; retain identification records for a minimum of five years

What Shufti Covers

Document verification, MRZ validation, and forensic authenticity checks address the identification and verification obligation. Stored decisions and exportable evidence support the record retention requirement. Ongoing monitoring and beneficial ownership verification require AML and KYB checks on.

6AMLD / AMLD4–5

Relevant Requirement:
Criminal law framework for money laundering offences and sanctions.Customer due diligence, enhanced measures for high-risk relationships, and audit-ready evidence of verification decisions

What Shufti Covers

Document Two supports EDD document collection for high-risk customers. Forensic evidence trails support audit readiness.

BSA / CIP & FinCEN CDD Rul

Relevant Requirement:
Collect, verify, and record identifying information for every customer

What Shufti Covers

Document capture, identity data extraction, and authenticity checks satisfy the verification and recordkeeping components of CIP.

UKGC

Relevant Requirement:
Verify customer identity and age before access; conduct affordability assessments for at-risk customers

What Shufti Covers

Identity verification, age confirmation, and Document Intelligence for affordability signals address the core requirements. Responsible gambling programme obligations.

Industry Use Cases

Banking & Finance

Audit-ready KYC across jurisdictions. Document Two for dual-document CDD. Document Intelligence for Income source identification. Single evidence trail for FinCEN, AMLA, and FINTRAC examination.

Crypto & Digital Assets

GenAI detection blocks synthetic IDs at submission. Tiered KYC via Journey Builder. Fraud Memory prevents account farming across exchanges.

Forex & CFD Trading

OCR deduplication catches variant accounts. Bonus abuse prevention via Fraud Memory. Document Two for MiFID II compliance and source-of-funds.

Gaming & iGaming

Document-derived age verification , DOB from the document, not self-reported. Affordability risk scoring via Document Intelligence. KJM certification for Germany.

Telecom

SIM swap defence via Video-Only mode. SIM farming detection via Fraud Memory. National SIM registration compliance across MEA, LATAM, and APAC.

Travel

MRZ/ICAO validation on every travel document. Continuous Verification for expiry monitoring. 250+ country coverage without per-route configuration.

Healthcare

Medical identity fraud detection. On-prem deployment for patient data sovereignty. Non-Latin OCR for cross-border telehealth populations.

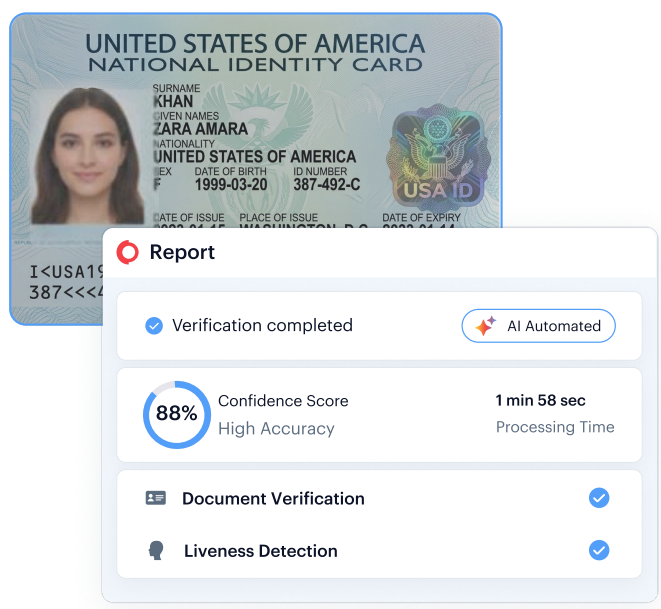
Digital Lending & BNPL

Document Intelligence Salary Analysis detects fabricated payslips before credit decisions. Sub-15-second decisions across risk tiers.

Delivery Models

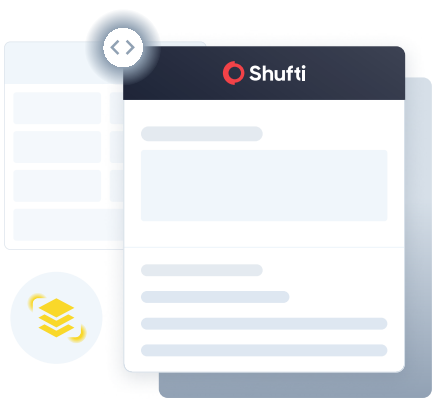
Verification Modes

- **Image DV**
  Standard KYC onboarding, account opening, age gating, seller verification
- **Video-Only DV,**
  Standard KYC onboarding, account opening, age gating, seller verification
- **Document Two**
  Dual-document compliance: EDD, source-of-funds, FATF CDD, AMLR



Integration Options

- **REST API**
  Submit documents, select checks, receive structured results with reason codes. Operational in days.
- **Mobile & Web SDKs**
  Guided capture with real-time quality prompts. Reduces retries before submission.
- **Back Office**
  Exception review with forensic signals and evidence pre-attached. Decisions stay audit-ready.
- **Journey Builder**
  Configure CDD/EDD flows per jurisdiction, risk tier, and event type without engineering rebuild. Standard users auto-approved. High-risk users routed to the right checks automatically.



Deployment Options

Cloud, On-Premises, or Hybrid. Full suite on your infrastructure for data residency requirements. PCI DSS certified. SOC 2, ISO 27001 certified. ETSI conformity in progress.

Every unverified document is an open door. Every RGB-only platform is blind to the AI-generated fraud already in your queue. Every aggregator dependency is a data sovereignty question your regulator will ask.

Sources

1. FTC, 2025; Thomson Reuters, 2023

Request a Blind Spot Audit

See Shufti's 9-layer forensic pipeline live against your document types and use case. Test your current stack against GenAI-generated documents, PVC reproductions, and replay attacks. See exactly what gets through. Talk to a Specialist , No pitch. Just answers for your compliance, fraud, and engineering teams.

www.shufti.com
sales@shufti.com

Book a Demo