Shufti

How Does The AI Works

Shufti offers digital identity verification solutions, employing AI and machine learning to streamline the verification process.

PCI DSS

SOC2

GDPR

QG GDPR

ISO 27001: 2013

CE+

iBeta Level 1

KJM AGE VERIFICATION

CCPA

Image Processing

Our system is designed to automate visual recognition tasks, enabling a computer to identify and distinguish various objects like human faces, lampposts, or statues, thereby replicating the observational skills of the human eye.

Machine Learning

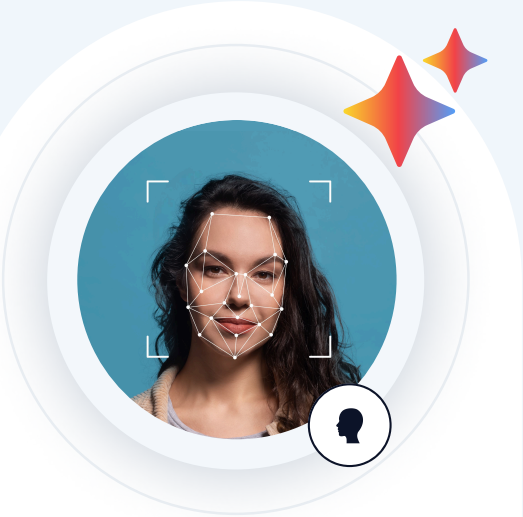
Our Machine Learning algorithm takes a dataset as input and learns from the data. It identifies the patterns in the data and provides the desired algorithm. For instance, to identify whose face is present in a given image, multiple things can be looked at as a pattern:

- Height/width of the face.
- Ratio of the height of the face to the width of the face.
- Color of the face.
- Eyebrows shape.
- Eyebrows shape.
- Width of other parts of the face like lips, nose, etc.

Anomaly Detection

Our AI models can detect any anomaly in the face verification process by doing the following checks:

- Checks for Face Screenshots.
- Assessment of Face Replay.
- Checks against 3D Face Masks.
- Deep Fakes Detection.



Operation in face verification

Face Detection

The AI model detects the presence and liveness of a face.

Image to Data Conversion

Facial attributes are transformed into a unique numerical code, termed as faceprint.

Match Finding

Faceprint is compared against images in documents or databases to identify and confirm a match accurately.

In the document verification process our AI works by checking the authenticity and integrity of the document.

Document Data Extraction

Our AI models, empowered with advanced OCR technology, are adaptable to any document type, extracting specific information from images. This capability allows organizations to streamline data entry processes and significantly reduce costs.
Common extracted data includes:

- Name
- Address
- DOB
- Gender
- Document Number
- Expiry Date

Signature Analysis

This involves examining the uploded file metadata, compression settings, and specific tags or sections unique to the software or vendor.

Metadata Consistency

Checking whether the metadata matches the usual document of its type and the modification details.

Specific Software or Camera Patterns

Identifies unique digital fingerprints from specific software or cameras.

Compression Anomalies

Looks for unusual compression signs suggesting editing, such as re saving or editing.

Excluding minor edits like cropping or resizing.

Integrity Detection

Pixel analysis focuses on identifying unusual areas in the image. It looks for inconsistencies in local features such as

Color Uniformity Check

Evaluates consistency in colors of the image to detect possible alterations.

Textual Consistency

Inspects edges of text and images for signs of tampering.

Resolution Consistency

Ensures uniform resolution across the document.

Integrity Detection

The uploaded document is compared against our AI model, trained on over 10,000+ global documents, to identify any inconsistencies effectively.

Document Comparison

Matches the authenticated document with AI models that are trained on original document templates.

Security Feature Verification

Checks for the presence of security features like watermarks, holograms and MRZ code.