Mobile Verify®

Scanner-optimized identity document verification

Since 1986, Mitek has been at the forefront of mobile capture and digital identity solutions for businesses around the world – using images captured from mobile devices to verify identities quickly and easily. Now, Mobile Verify leverages that same industry leading technology to analyze ID documents captured on scanners.

Authenticity elements evaluated

1. Document Structure
2. Biographical Data
3. PDF417 Barcode (if applicable)
4. Mechine Readable Zone (if applicable)
5. Security Features
6. Portrait Zone
7. Signature

How it works

Mobile Verify uses AI and machine learning to evaluate identity documents captured on common scanners to ensure documents scanned are genuine and unaltered.

Classifying identity documents

After an identity document image has been captured, it is submitted via an API call to Mobile Verify. Then, proprietary AI and machine learning algorithms automatically classify the document by matching it to a template in a cloud-based repository. Matching ID documents to known templates is the first step in validating the authenticity of the document presented. Mitek maintains a proprietary and expansive cloud-based repository with thousands of identity document templates from around the world with new templates continuously added. Results returned to customers will reflect whether the document matched a template in the repository. Documents presented that do not match a template on file are handled at the customer's discretion. If an unmatched ID document is determined to be a valid template that is actively used, it can be queued by Mitek for future development and added for automated classification.

Extracting data and initial checks

Through a combination of computer vision techniques, optical character recognition (OCR) and rules, Mobile Verify compares the structure of the ID to a corresponding template. It analyzes components such as the biographical information, signature block, portrait area, machine readable zone (MRZ), and barcode to ensure they match. Extracting information from these elements, Mobile Verify then checks to make sure the ID data is consistent, and that the data encoded into the MRZ, and barcode, match the biographical information printed on the document.

Gathering evidence

To further determine if the ID document is original and unaltered, Mobile Verify releases its proprietary analytic models to examine the ID for alterations and other suspicious indicators using deep learning techniques detailed below.

Computer vision (CV) algorithms evaluate details like the overall structure of the ID document, photocopy indicators or elements pointing to digital alterations (such as a portrait being digitally generated). They also examine the image quality, very low or very high can both be red flags. These algorithms are constantly evolving based on the hundreds of thousands of ID documents that Mitek processes every year for customers around the globe.

Machine learning (ML) algorithms scrutinize the ID for a wide range of characteristics, such as font usage and consistency. Utilizing Mitek's repository, the algorithms are trained to spot an enormous set of identified characteristics of both forged and legitimate ID documents. Going beyond individual ML forensic checks, the use of Ensemble ML techniques is equivalent to simultaneously running hundreds of forensic check permutations.

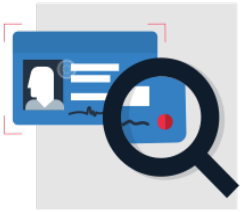
Deep learning algorithms (DL) can find subtle problems with IDs, such as slight irregularities appearing on or between certain letters. They are trained to identify problematic features on their own by analysing massive quantities of IDs labelled as "genuine" or "forged/counterfeited."

Weighting evidence

Each of the evidence-gathering algorithms output a fractional score between 0 and 1 (with zero representing highest risk and 1 representing lowest risk) — most scores falling in "gray zones" between the two. This range of values is more accurate and nuanced than a simple binary result would be, but it creates an immense challenge when combining these gradations of score values into a single definitive answer.

Using techniques based on rules for determining minimum values or allowable ranges, the result would be a loss of accuracy and nuance. Therefore, a more intelligent analytic approach is needed.

Mobile Verify uses an additional level of machine learning to examine all the outputs from the evidence gathered. This higher-level ML decides how much weight (relative importance) to give each point of evidence based on everything discovered about the ID being examined and everything known about the genuine and counterfeited IDs in the repository. It is an immensely complex task, but Mobile Verify performs it in seconds.



Optimization for scanned documents

There are several key differences to be aware of when utilizing images captured from a scanner versus those captured on mobile devices. These differences include:

- Controlled acquisition such as color and lighting
- Lack of distortions
- Higher resolution

Mobile Verify addresses these differentials in a scanner specific authenticator, uniquely designed to detect color photocopies using scanners. The evaluation algorithms for scanned documents have also been optimized specifically for scanned images as an input, and scoring models have been tailored to determine that ID documents are genuine and unaltered.

General scanner setting guidance

To optimize scanner image processing using Mobile Verify, the following settings are recommended to improve results.

Color settings:

- "True Color" or similar color configuration as applicable to each device
- Disable scanning at non-visible frequencies (e.g. UV, infrared)

Quality settings:

- JPG image format at 90-95% quality (low compression)
- 600 dpi
  - » If 600 dpi is not possible with your device, we may be able to accommodate a lower setting. However, setting the resolution as low as 300 dpi may not render barcodes clearly enough to be read.

Other settings:

- Disable any options that add an artificial frame to the image.
- Some identity documents include a transparent window. If your device includes a "hole filtering" option, set this to its maximum value. Doing so ensures the device will not mistake the window with the end of the document.

Optimized for Mobile Verify

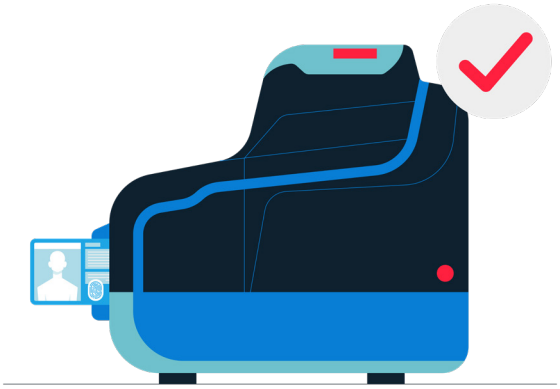
Mitek has evaluated various scanners from different providers to assess Mobile Verify compatibility.

Check with your scanner provider to optimize your settings for Mobile Verify.

Mobile Verify ensures

99.995%

system uptime, is cloud-based and offers enterprise grade security including mutual authentication (MA), message level encryption with RSA, and SOC 2 Type 2 compliance.



To learn more about using Mobile Verify for your scanned ID documents, visit us today at www.miteksystems.com

Mitek

About Mitek

Mitek (NASDAQ: MITK) is a global leader in digital access, founded to bridge the physical and digital worlds. Mitek's advanced identity verification technologies and global platform make digital access faster and more secure than ever, providing companies new levels of control, deployment ease and operation, while protecting the entire customer journey. Trusted by 99% of U.S. banks for mobile check deposits and 7,900 of the world's largest organizations, Mitek helps companies reduce risk and meet regulatory requirements. Learn more at www.miteksystems.com.