IN-D

Getting started with IN-D.AI

Document Fraud Detection

Functional Overview

Date	Version	Document Changes
03-03-2022	1.0	First copy
07-03-2022	2.0	Review Comments Incorporated

Contents

Introduction

Verifying the identity of any individual whether a customer, partner or an employee has always been a prerequisite for all businesses. Most of us have experienced this during an account opening, where a person is required to submit a govt-issued ID document, a verification officer manually verifies the details on the ID document to make sure that the person is not an impersonator.

As digital workflows grow, organizations have started using [Identity Verification Solutions](#) to process, authenticate and verify these identities at scale. This gave an opportunity to fraudsters to create fake documents and allow someone to claim the identity of another person. Moreover, online transactions have jumped due to the change in behaviour induced by COVID-19 making the use of Fake IDs a burning issue that needs immediate attention.

With the advancement in AI technologies, technology can now help in detecting and eliminating these Identity frauds or Forgery. An AI based Fraud Detection solution analyzes the unique information contained in the identity documents to check their validity, then ensures that the details appearing in the workflow is identical to that of the identity document, so that only the authorized person can access the services.

Types of ID Document Fraud?

Here are a few categories of document fraud that fraudsters use to fake the identity.

Completely Fake documents

As name suggested these documents are false documents. They are built to look like real documents but lack the characteristics of original documents such as QR Codes or placing of certain landmarks such as national emblem etc

False Documents

False documents aren't forged or manipulated documents, but they are physically stolen documents that fraudsters use to bypass the document verification. Intuitively its understood that an AI based ID Fraud detection system will not be able to weed out such documents but there are other techniques available such as Face Match and Liveness Detection to help prevent such frauds.

Modified Documents

These are original documents that have been altered to fool the verification. Most of the modified documents are created by fraudsters in such a way that it becomes difficult for humans to identify any alterations. These are the most predominant type of fake documents that fraudsters use to trick the system.

How AI Document Verification Works?

AI-enabled ID document verification solutions test various elements of the ID documents while verifying the authenticity of the said ID Card. Some of these checks are done in the image domain using Computer Vision techniques, which can detect even if it is a slightest change in a single pixel, and some checks are done in the text domain using Optical Character Recognition (OCR) techniques.

Card Edit Checks

These types of checks are applicable for all types of fraudulent ID cards. AI and machine learning models for these checks make sure that the documents submitted have not been tampered for any textual information contained in it such as Name, DOB, ID Number etc. These Text level fraud checks involves identifying legal characters, measuring inter-character spacing, measuring inter-line spacing and new-line characters, font-check, and text-color check etc.

Face Morphing and Face Editing

Face Edit Checks for any alterations of original personal photograph on an ID Card using various photoshop software. These checks are predominantly used by fraudsters to bypass face-matching checks done against a selfie either by software or verification agents.

Face morphing is a new sophisticated kind of fraud where two photos with facial similarities can be superimposed to create a fake photo. Face morphing can be employed to assign multiple identities to a single photo.

Format Identification Checks

AI-based solutions can identify the exact format of the documents. Upon training on a particular document format, AI models are capable of accurately detecting any signs of forgery with respect to the exact format of the document and check for crumpled or folded documents. These checks are very relevant on Identifying completely fake ID documents.

Landmark Detection

All Government-issued identity documents contains some special types of identification marks such as holograms, QR Codes, National emblems, Placement of Signatures, Photos etc. These landmark detection checks can detect, First, the presence of these landmarks on that document type and, second, in case of any change or tempering the placement of these landmarks viz a viz original known positional co-ordinate.

Authenticating MRZ or QR Codes

AI checks the availability of the machine-readable zone (MRZ) and QR Codes on the document and matches it against the information on the document.

Checking the micro prints

Some Government-issued ID documents have microprint as an additional security layer to prevent fraud. The AI checks microprinting for authenticating documents.

IN-D's Solution for Indian Identity Cards Verification

Introduction

IN-D's Fraud Detection module is part of the overall Identity Verification Solution that can identify fake documents and more importantly modified ID documents for signs of forgery or tampering. AI models trained for this purpose are capable of accurately detecting any signs of forgery through Photoshop and can detect even if there is a slightest change in a single pixel, which is very difficult to detect even with the naked human eye.

IDs Processed

The solution currently handles following major Indian ID documents

1. Aadhar Card Front
2. Aadhar Card Back
3. PAN Card
4. Voter ID
5. Passport Front
6. Passport Back
7. Driving License

Types of Checks Available

Table below lists the checks currently available with the IN-D solution and their accuracies on sample image dataset available with IN-D.

Check type	Document(s)	Current Accuracy
Card Edit	PAN	80%
Face edit check	Aadhar Card Front, Voter ID, Passport Front, Driving License, PAN Card	90 %
Face Morphing	Aadhar Card Front, Voter ID, Passport Front, Driving License, PAN Card	80%
Landmark Detection		
i. Face detection	Aadhar Card Front, Voter ID, Passport Front, Driving License, PAN Card	90%
ii. QR code detection	Aadhar Card Front, Aadhar Card Back, PAN Card	85%
iii. Signature detection	Passport Front, Driving License, PAN Card, Cancelled cheque	90%
iv. Logo detection	Aadhar Card Front, Voter ID, Driving License, PAN Card	90%

All the checks return confidence scores along with coordinate information for the detected objects, both of which can be used for the post-processing of results as applicable. Furthermore, deep learning techniques allow for processing of even hard to parse documents like zoomed-in, skewed, multiple documents in one-page, full-page Indian Aadhaar card, photocopy, and greyscale images.

Technical Overview

The IN-D KYC fraud detection model can be deployed on-cloud and on-premises, thereby addressing security and cost concerns. The technology is available for the major Indian ID cards and can be extended to ID cards of various continents.

The IN-D KYC fraud detection module uses Python for programming and the Keras library with Tensorflow as a backend for deep learning studies. The hyperparameters for model training and data augmentation are customized by IN-D for the use case.

Benefits of using AI for document verification

As digital workflows grow, verifying the identity of the customer becomes more and more important. ID document Verification helps organizations reduces business risks, reduce fraudulent losses, save their customers, and helps in compliance with local regulations KYC – Know Your Customer regulations, all automatically and generating near zero errors when combined with manual processes.

ID document Verification works behind the scenes to ensure that only valid ID is recognized.

Concluding Remarks

Many solutions for document fraud detection exist in the literature. The IN-D KYC fraud detection module is unique in that it combines creativity, ease of use (training and testing), low latency and high accuracy in one model. Just as a human can detect ID document fraud by only looking at the templates, fields, and the color scheme, similarly a machine can be trained to detect ID document fraud in the text / image domain. Most importantly, new categories (of different aspect ratios) can be added without the tedious job of going through each sample. IN-D believes in research and innovation and this model is an exemplar of this ideology.

IN-D models are trainable and hence can be used to improve performance as more samples are encountered. The models clearly explain the possible cause(s) of failure along with providing the confidence score for each model / feature. The institutions can set up appropriate confidence thresholds based on experiments / heuristics in consultation with IN-D. Object detection and image-based techniques enable us to detect frauds where purely text-based methods fail. Implementation of fraud detection methods in the ID verification process results in reduced costs, better classification & digitization accuracies, and efficient systems.

Industry players who are looking for an innovative and accurate solution for their digital Identity Verification processes will find the solution useful.