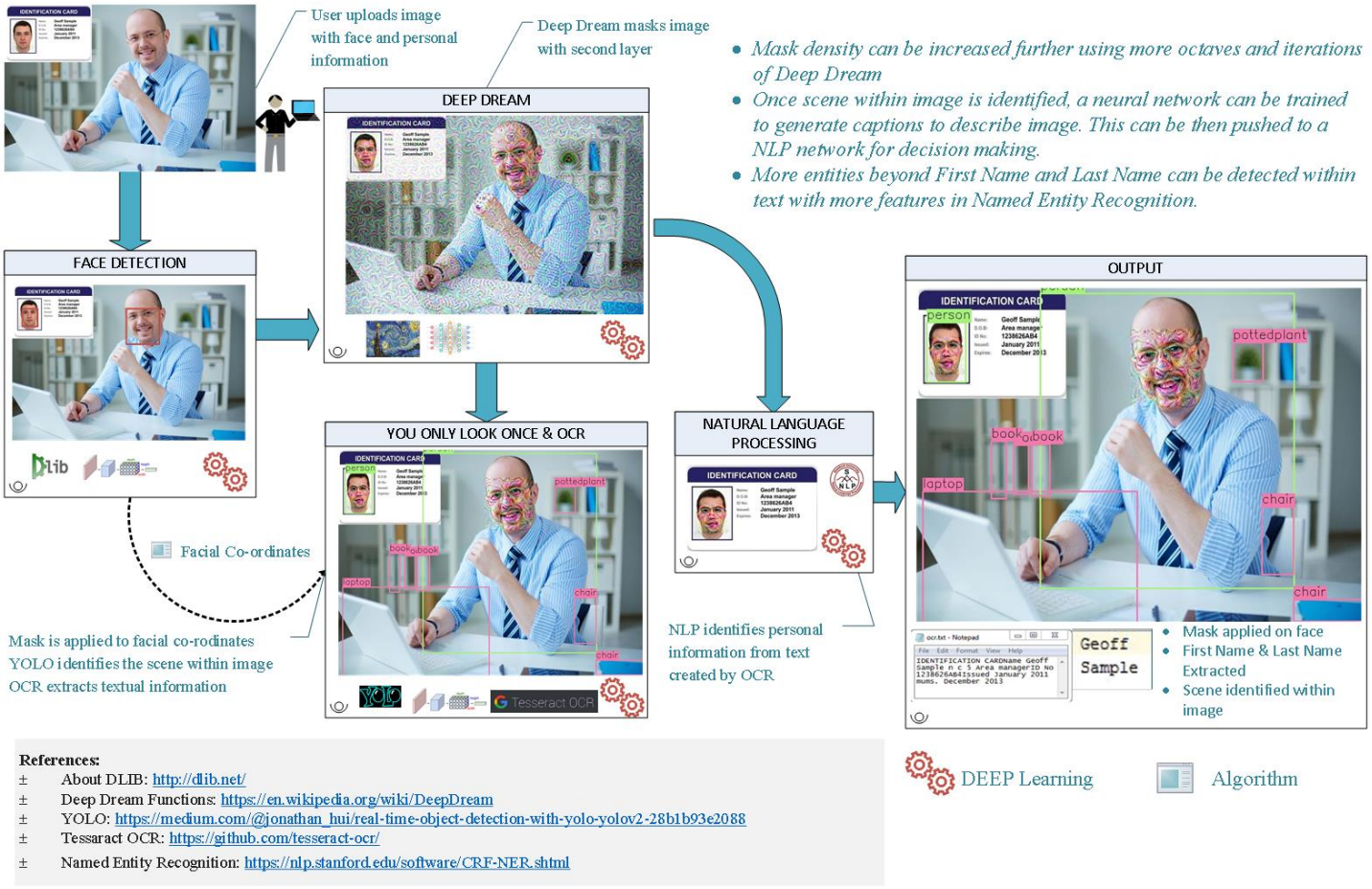
Deep Learning: Detect & Mask Personal Information In Documents



PII compliances mandate organizations to protect personal data. Detecting PII within image which may contain individual's Face, ID & Objects is challenging.

Deep learning concepts mentioned below are used to overcome this challenge:

- Convolutional Neural Network (CNN) – Detect face in document
- You Only Look Once (YOLO) – Detect scene in document
- Deep Dream – Mask personal information in document
- Optical Character Recognition (OCR) – Detect text in document
- Natural Language Processing (NLP) – Detect personal information in text

Face is detected through DLib library, linear SVM and CNN (*with 58 facial co-ordinates*). It returns 128-dimension face encoding vector. Custom model can be created by re-training CNN instead of using DLib.

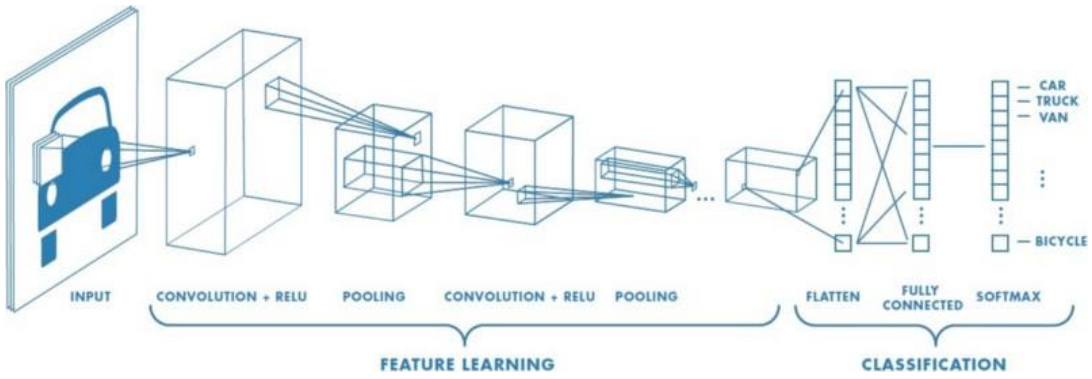


Figure 1: Typical CNN Architecture

Deep dream enhances patterns and creates psychedelic image. It can be used to mask the personal information (*viz. Face*). This model uses Octave=2 and Iterations = 100 with scope of further scaling-up for more obfuscation.

YOLO identifies all the different objects present in the image. It helps in identifying information of the scene within image to generate captions using NLP & evaluate further.

Optical character recognition(OCR) is a technique which transforms mechanical or electrically typed texts into machine encoded texts. Tesseract OCR, which is an open source API or any other open source tool may be used.

Natural Language Processing(NLP) analyzes human language and can identify the semantics present within text. Here Stanford Named Entity Recognition NLP is used to identify first name and last name.