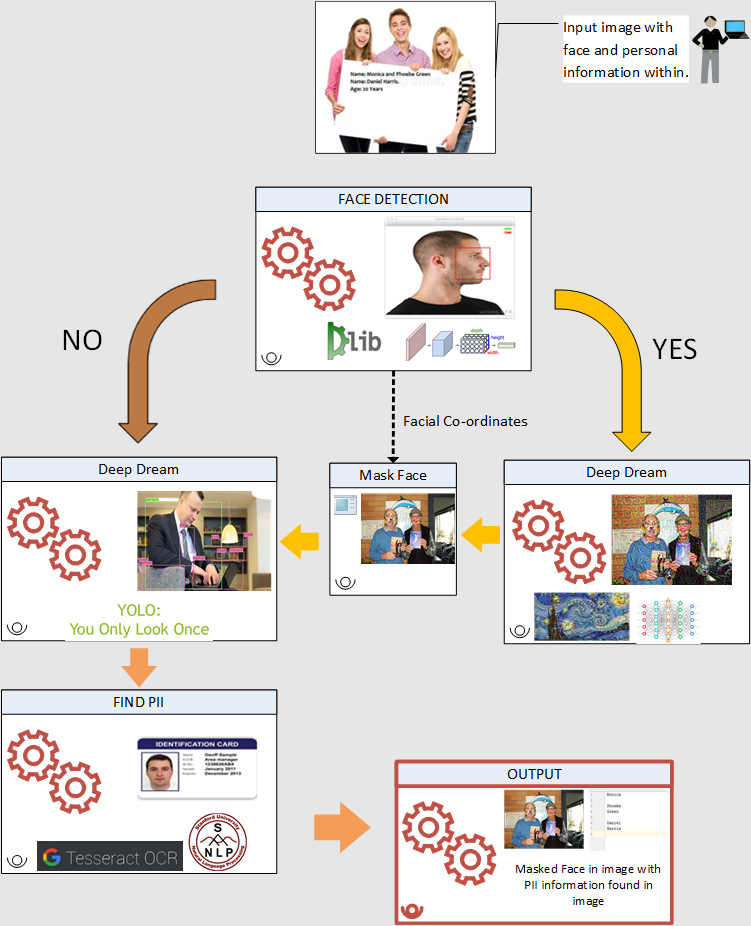
Detect PII Within Image For GDPR Compliance

Information Technology Solutions

## Face Recognition API

Face is detected using face\_recognition package in Python, which mainly uses DLib as a reference library. Image, then, is obfuscated using Google’s Deep Dream API. It first loads an image into a numpy array, and then finds the face encodings. These encodings can be compared with other images to see whether image is matched or not. Face encodings return a 128 dimension face encoding of each face in an image.



## Overall Process:

GDPR stands for General Data Protection Regulation, which a rule adopted by EU Parliament on April 16th, 2018. This rule mainly gives an individual to a right to control their personal data. This obliges the companies under EU Governance to protect their employees’ personal data under any security breach and failing to do so, companies would have to face penalties and other consequences.

One of the challeges in identifying personal information is when images of individuals are contained in a document or when personal information (like names) is within the image. Our approach is to make a system that can accurately classify this personal information which is present in a document without human intervention. To do so, we employed the use of various Deep learning concepts.

Scope of this work is to detect:

* Face of individual within image
* Classify other objects shown within image
* Personal information like First Name & Last name

This system can be further fine tuned to be more elaborative.

In this approach, we try to detect personal information in an image by detecting human faces and recognizing names inside it. We start by detecting human faces in an image, which is obfuscated using Google’s Deep Dream API. Other objects in that image are, then, identified using YOLO. Text in that image is detected with Optical Character Recognition (OCR), and person’s names are identified by implementing Stanford NLP’s Named Entity Recognition (NER).

Prepared By : Neel Parikh, Tirth Thakkar

Guidance By: Dhaval Mandalia

Abstract

General Data Protection Regulation (GDPR) states that all the companies must provide a reasonable data protection for personal data of their customers. Personal Data includes any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a home address, a photo, an email address, bank details, posts on [social networking websites](https://en.wikipedia.org/wiki/Social_networking_service), medical information, or a computer's [IP address](https://en.wikipedia.org/wiki/IP_address). In this approach, we cater to design a system which can detect and/or mask personal information of an individual like First Name & Last Name, and facial image through which individual can be identified. Addtionally this system also detects other objects within the image which can be manually reviewed for any personal impressions.

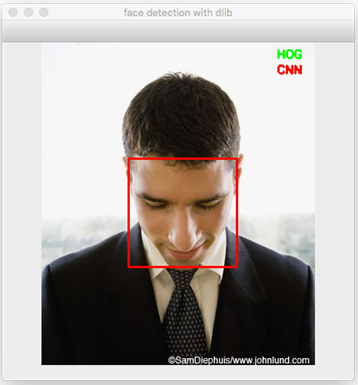
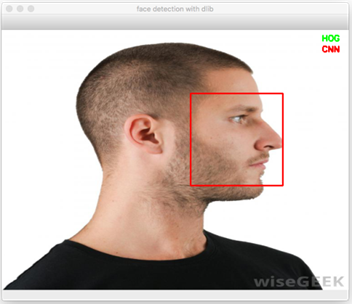
We have detected face in given images and obfuscated them by using Google’s Deep Dream algorithm, objects within the same image are detected using YOLO algorithm & Textual information using Stanford NLP’s Named Entity Recognition (NER).

Ref: Convolutional Neural Networks (CNN), Deep Dream, Named Entity Recognition (NER), Natural Language Processing (NLP), You Only Look Once (YOLO).

## DLib

DLib is a C++ based toolkit that contains machine learning algorithms to solve real world problems. The frontal face detector in dlib is based on histogram of oriented gradients(HOG) and linear SVM. DLib also provides CNN based face detector which can detect faces almost in all angles. While the hog based face detector takes less time, CNN based face detector would take considerably more time. However, the results show much more accuracy for CNN based face detector.

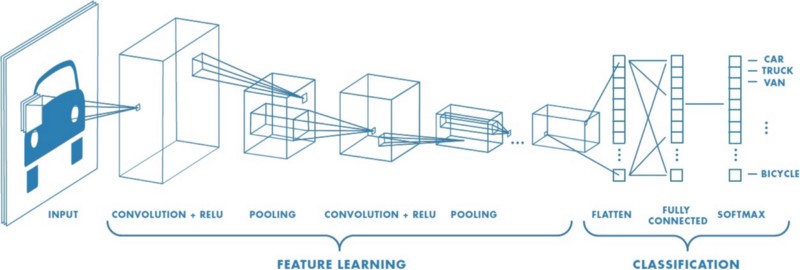
*Fig 1. Face detection*



## Deep Dream

Deep dream is a Google API that uses CNN to find and enhance patterns in images and create psychedelic image from that. Deep Dream mainly reverses its neural network. When any random image is given and told to find an object that is not present in an image, rather than failing to find the object, the system starts to recreate image in a way that it finds the object it was supposed to identify. Thus, it creates a hallucinating image. In practical implementation, lower level layers identifies the edges of the object, and as layers are increased, patterns are created into an object shape which are overlapped repeatedly to create a hallucinating image. The model used in this process uses Octave=2 and Iteration = 100. They can be further scaled up as per requirement to give more obfuscation . An image before and after applying deep dream would look like following:

*Fig.2* *Convolutional Neural Networks*



## Convolutional Neural Network(CNN)

Convolutional Neural Network(CNN) is one of the main categories of image classification and recognition. CNN mainly trains a model from a set of input data that is used for detecting a specific entity in an image. CNN has different layers, like convolution, ReLU, max pooling etc. Convolution layer extracts features from an input image. ReLU basically introduces non-linearity in the network. Pooling is used to reduce the size of an image so that operations can be performed faster. . A sigmoid function, for example, would have the following equation:

S(x) = 1/(1+) (1)

A simple CNN process would look like following: