Machine Learning Engineer Capstone Proposal

Bruno Bitencourt Luiz
June 9th, 2019

Early Threat Detection and Object Recognition with Generative Adversarial Networks

## Domain background

Airports security is tested each day by passengers from all around the world. Before entering a plane, the passenger and his luggage should be inspected to search for items that can harm other people or compromise flight security. This kind of inspection is made by scanning passengers body and luggage using x-ray techniques.

In most airports, each year the number of passengers increase and together, the number of illegal items that are apprehended. In 2018, the Guarulhos Airport in Brazil received almost 15 million[1] people from international flights and make 292 arrests. The majority of arrests are for drug traffic and other illegal items such as guns, knives, and other items. The luggage inspection is made when the baggage is being dispatched before the takeoff and on the arrival. Also, during terminals transportation.

Identifying threats is the most important thing to do. But object discrimination with x-ray can be very helpful. Especially, to reduce the estrangement of a passenger by having to open your luggage in front of the police. This can be used to identify if the passenger has a suspicious amount of items in his luggage, such as watches, shoes, glasses, etc.

The majority of systems in this field are closed and not share any dataset. Some of them, like ALERT[2], offers a dataset to sell, but if you buy it, you can’t share with your project.

By working in this task we can improve the precision of object detection and also, provide inspiration for many objectives such as identifying threats in schools or small airports. Also, some aspects of the model can be applied to improve further works on x-ray interpretation for medical reasons, for example, wrong pathology diagnosis[3].

[1] Guarulhos International Airport - Operational Info
[2] ALERT Datasets
[3] Cross-Modal Machine Learning as a way to prevent improper pathology diagnostics

## Problem statement

This problem can be framed with Deep Learning since we will use deep neural networks and imaging processing in many different ways.

In terms of imaging, we have an image classification with segmentation task, were in our dataset we have areas at the image where some items are illegal, others not. For example, baggage with normal stuff, like a phone, glasses, a wallet, and in a pocket may contain an illegal item like a fire weapon.

With the lack of data images showing dangerous items, we can apply Generative Adversarial Networks (GANs), in which we generate a set of images to improve the number of our samples and also increase our precision by using discriminative classifiers.
In summary, I will use:

- Deep Learning
- Image Classification
- Image Segmentation
- GANs - Discriminative and Generative

## Datasets and inputs

As mentioned before, acquiring this kind of data is not an easy task. In the end, I've found the dataset "*GDXray: X-ray images for X-ray testing and Computer Vision"* published by professor Domingo Mery[4]. The dataset has 2.9GB of baggage images containing dangerous items such as guns, knives, and non-dangerous items such as phones, keys, notebooks, and so on. This dataset contains more than 19 thousand black/white x-ray images, but only a few samples are from items on baggage or backpacks.
The GDXray has 5 different datasets on it. For this work, I will only use the Baggages dataset. In total, we have 8.950 grayscale images separated on 77 folders, where each folder correspond to a series. There are 600 images of displaying mixture fire weapons, shurikens, and razor blades. Additionally, 576 images of knives in various positions, 178 images of a backpack with a gun with various angles, and many small series of backpacks

[4] GDXray Dataset

with illegal items. This dataset lacks samples of baggage without any dangerous material. In the end, I will only use around 1.500 images from this dataset, since the normal samples are too random.

Another dataset that I will be using is the SIXray from University of Chinese Academy of Sciences (UCAS-PRISDL)[5]. This dataset contains more than 1 million images and almost 9 thousand of samples from dangerous items, in approximately 72GB.

SIXray has samples from color x-rays, witch different colors for different materials. In this dataset there are 1.059.231 images, being 8.929 samples from baggage containing illegal items. That means this dataset is unbalanced, only 0.84% of the samples have the kind of items we are trying to detect.

There are 6 classes of illegal items: 3.131 images of guns, 1.943 knives, 2.199 wrenches, 3.961 pliers, 983 scissors, and only 60 hammers.

There will exist 2 models for this task. One model will learn from GDXray, which differs a lot from SIXray. Further, I will use this model as a layer to the second one, obtained from SIXray dataset and see how it helps with our classification. Our main goal and final metrics will be evaluated from the SIXray dataset since it’s the most real one. But the first model also will be evaluated before I can use as transfer learning.

The SIXray paper shows us that the best results are achieved by using at least 1/10 proportion. I will stay around 5% and 30% of samples of illegal items. It's not easy to define an exact number before experimenting and done some validation while working with this large dataset. There are many calibration steps that may require small adjustments during the project.[6]
For both datasets, I will use 70% for training, 15% to test and 15% for validation.

### Solution statement

The main goal is to *classify* an image as containing a dangerous object or not. Using Deep Learning I will use a Convolutional Neural Network since we need to classify and do

[5] SIXray Dataset
[6] 37 Reasons why your Neural Network is not working

segmentation of the objects. This kind of NN transforms the image pixels on features, witch them are split into several additional layers. By using transfer learning from the first model, we can define how further improvements can be done to simplify the training process or even achieve better results.

Since both datasets have some challenges, one strategy that I will use is a GAN. Since a GAN can be used to explore a weakness in our discriminator, we can improve in some aspects like handle overlapping, which is a big issue. Another aspect that we can benefit is by using generative as a solution for the lack of data if data augmentation doesn't work.

For this type of classification, our first metric will be *recall* since its more important don't miss a dangerous object than triggering a false alarm. Another important metric is the IoU (Intersection over Union), where we will have the precision of an item, by calculating the intersection of the predict object region and the ground truth (real position).

**Benchmark model**

A good comparison with this project are the results from the paper: "*SIXray: A Large-scale Security Inspection X-ray Benchmark for Prohibited Item Discovery in Overlapping Images*[7]*"*. This article produced the SIXray dataset and applies a technique called class-balanced hierarchical refinement (CHR) to evaluate the precision of identifying threats.

We could use the final results using the proportion of 10 nondangerous items to one dangerous, which has achieved an average precision of 77.2%.

**Evaluation metrics**

The metrics that I'm going to use are precision and recall. The success of the solution can be measured by achieving a precision greater than 77.2%. Personally, at the final model, I expect a recall for each object (guns, knives, wrenches, pliers, and scissors) with at least 70%.

[7] *SIXray: A Large-scale Security Inspection X-ray Benchmark for Prohibited Item Discovery in Overlapping Images*

**Project design**

The first thing on starting with the project will be data preprocessing and labeling. I will be using samples of dangerous items from both datasets. For the nondangerous, I will take only from SIXRay, since on GDXray these items are alone in the image. Thus, I can label all the samples as dangerous or not dangerous. By using these two datasets I will have samples with shape well defined from GDXray and with overlapping from SIXray. During the benchmark, I will test with a hidden layer trained with just GDXray and check how it performs. Also, by using transfer learning, I will test with a layer trained with normal objects and see if we can improve our model.

After gathering an overview, I will proceed by optimizing the model. In the end, I will have the strengths and weakness of the model. I've presumed some image manipulation will be needed such as color filtering, rotation, etc. My intent is to document each experiment and results until the final result.

**Resources that I'm planning to use**: Python 3, pandas, sci-kit learn, OpenCV, Tensorflow, Keras, Seaborn, Matplotlib, Jupyter Notebook.

**FIG 1**: Random visualization generated from samples of both classes (GDXray)

Dangerous items are images containing at least one illegal item.

Safe items are the images not containing any illegal item.

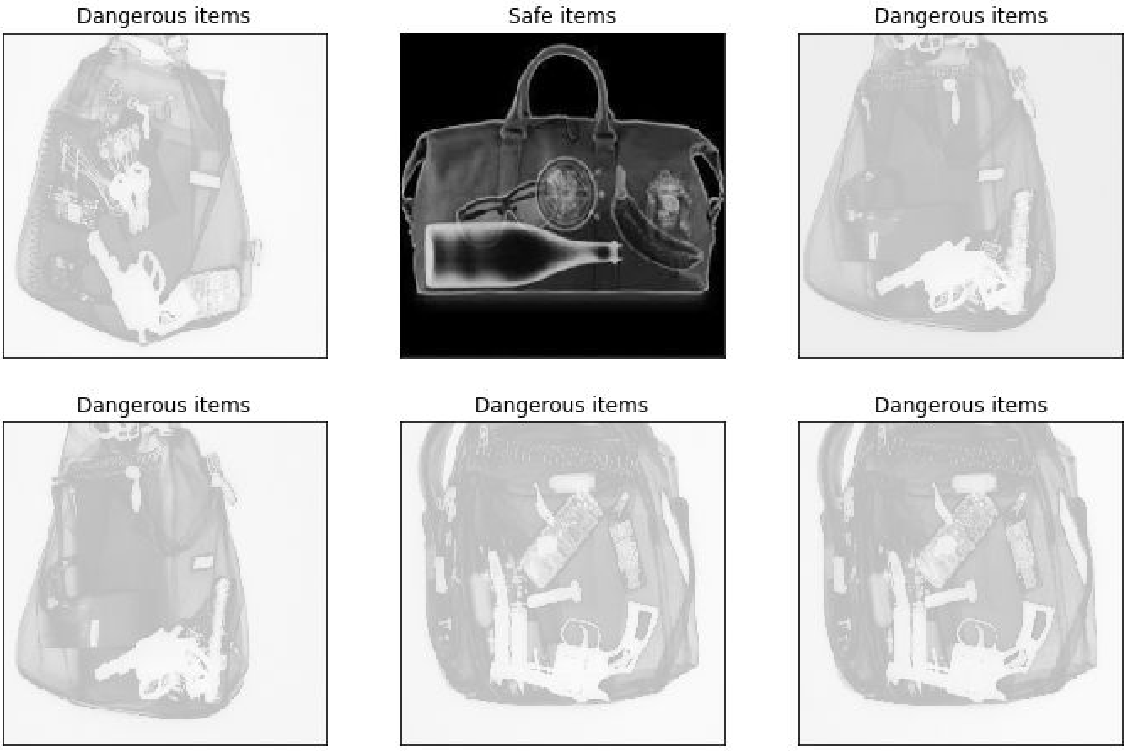

**FIG 2**: A backpack with a notebook and a gun (SIXray)