Machine Learning Engineer Nanodegree

Capstone Proposal

Domain Background

I believe everyone hates the CAPTCHA, the text images mixed with text, we have to type in before accessing webs or logining accounts. The purpose of CAPTCHA is make sure we are real person and prevent the computer from automatcally logining in. My inspiration is from the MNINST and SVHN datasets.The concepts are the same.

Although more and more websites change their defend system form CAPTCHA to others, lots of websites,including government's sites, still use the CAPTHA. By this capstone, I want to reveal that even beginner as I can easily solve CAPTCHA. it is not only easy to machine to solve, but it annoy human users a lot. Baes on the study :"How Good are Humans at Solving CAPTCHAs? A Large Scale Evaluation". it revealed that it is more effective for an attacker touse Mechanical Turk to solve captchas than an underground service. chrome-extension://oemmndcbldboiebfnladdacbdfmadadm/https://web.stanford.edu/~jurafsky/burszstein_2010_captcha.pd

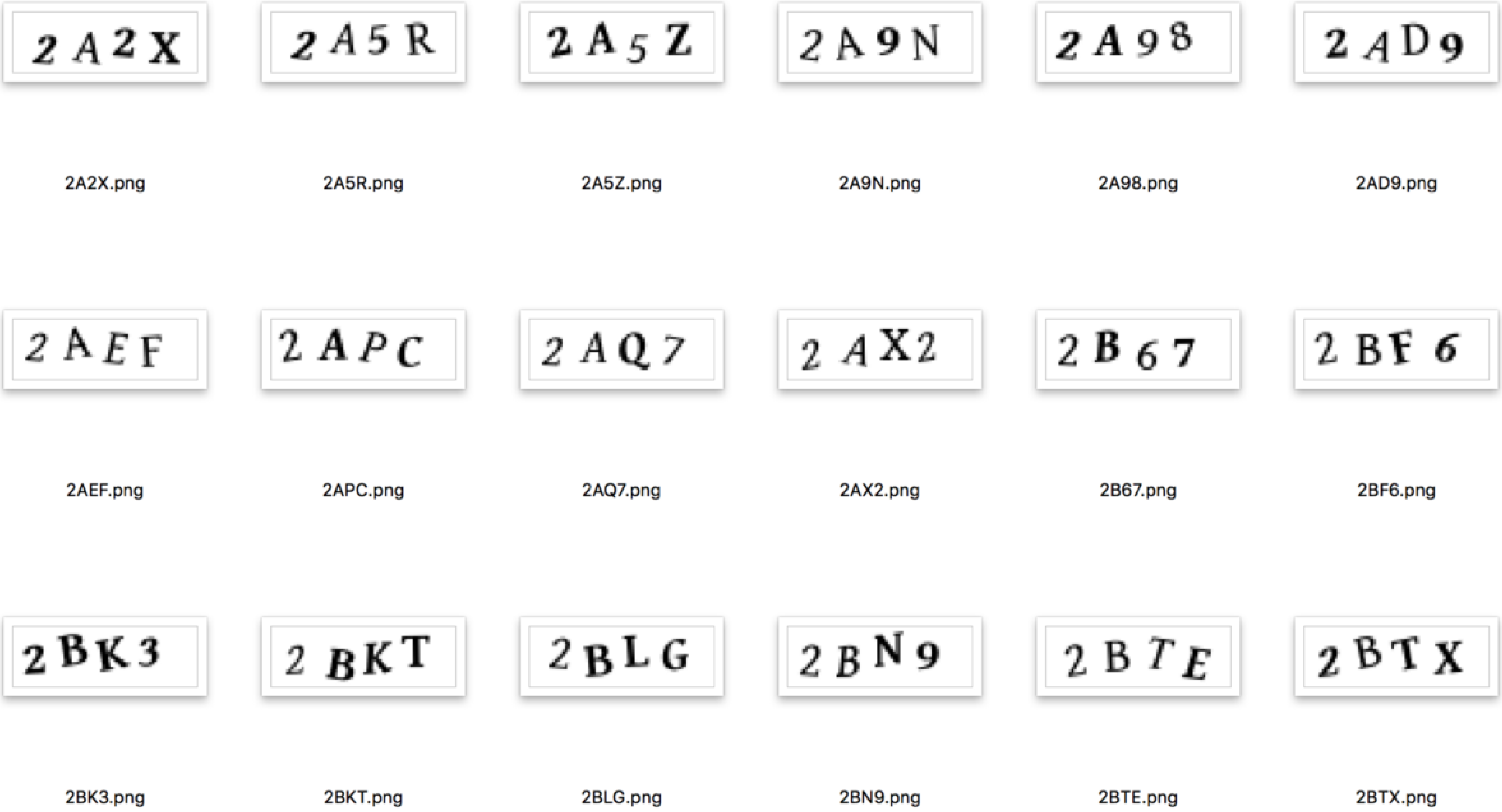
Problem Statement

Use the computer vision to recognize and break the CAPTCHAs, and evaluate how accuracy the model can do by teseting different kinds of images.

Datasets and Inputs

To break the CAPTCHAs, we need to tons of images to train our mode to manually solve them. Fortunately, I found the CAPTCHA samples iamges from the https://captcha.com/captcha-examples.html

```
In [15]: from IPython.display import Image
         Image(filename = 'C:\\Users\\MLUSER\\Documents\\GitHub\\Udacity\\2A5R.PNG')
```



2A2X.png 2A5R.png 2A5Z.png 2A9N.png 2A98.png 2AD9.png

2AEF.png 2APC.png 2AQ7.png 2AX2.png 2B67.png 2BF6.png

2BK3.png 2BKT.png 2BLG.png 2BN9.png 2BTE.png 2BTX.png

Solution Statement

I will use Deep Learning to solve this problem. The reason is that the images features are easy to extracted, by the white backgrounds of all images. Specifically, I will use CNN, which are effective at finding pattrerns by using filters to find specific pixels grouping.

Benchmark Model

I plan to use MLP as bechmark models to compare the CNN. The methods are like the MLND projects "cifar10_mlp" and "cifar10_cnn".

Evaluation Metrics

The evalustion metrics is simple that I will compare the accuracy of MLP and CNN. the coorect classification of images divide the whole datasets

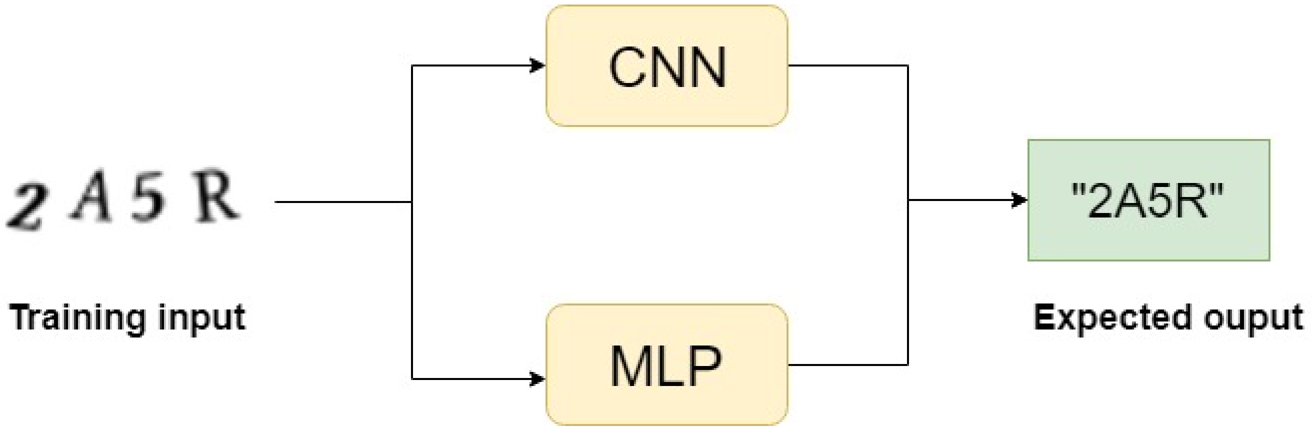
Project Design

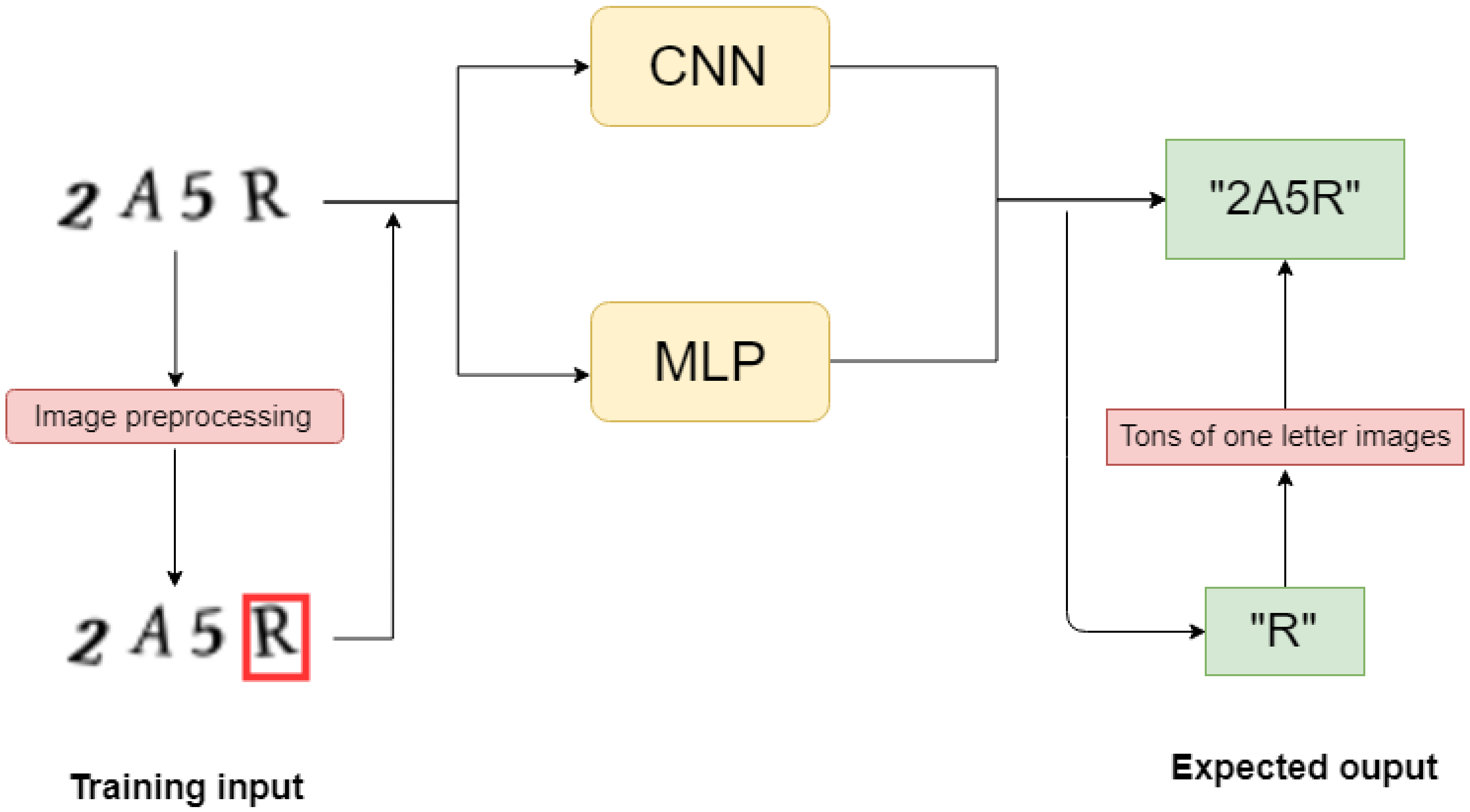
My traing data as below are images with random four letters, numbers and characters. the images files are named as their contents. However, we can find that images with four latters can be split to one letter, then we can use one letter image to train our model. it will reduce our computational time. Therefore, In image preprocessing, I use findContours() of OpenCV function to split the boundaries of each letter in each image. Then I extract individual letters from images I have and save each letter in it's own folder. So with images preprocessing, our working flow is modified as below.

The strategy I used is two Convolutional layers with two MaxPooling layers and two fully-connected layers(Dense), one is hidden layer and the others is output layer. I used the Multiply layer perceptron(MLP) as the benchmark model. the architecture as below is two fully-connected layers with two drop out layers.

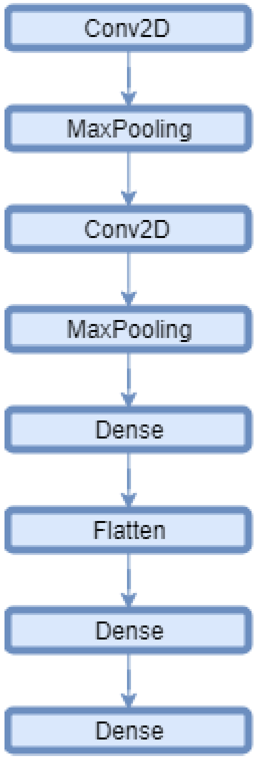
In [34]:

```
from IPython.display import Image
import nbconvert
display (
Image(filename = 'C:\\Users\\MLUSER\\Documents\\GitHub\\Udacity\\flow diagram.jpg'),
Image(filename = 'C:\\Users\\MLUSER\\Documents\\GitHub\\Udacity\\flow diagram (9).png')
)
```

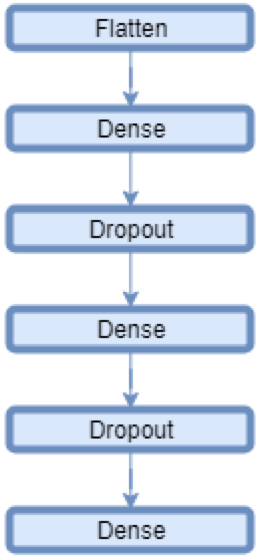




In [29]:
```
Image(filename = 'C:\\Users\\MLUSER\\Documents\\GitHub\\Udacity\\flow diagram (6).png')
```



CNN



MLP

Before submitting your proposal, ask yourself. . .

- Does the proposal you have written follow a well-organized structure similar to that of the project template?
- Is each section (particularly **Solution Statement** and **Project Design**) written in a clear, concise and specific fashion? Are there any ambiguous terms or phrases that need clarification?
- Would the intended audience of your project be able to understand your proposal?
- Have you properly proofread your proposal to assure there are minimal grammatical and spelling mistakes?
- Are all the resources used for this project correctly cited and referenced?

```
In [ ]:
```