Summary
- CAPTCHA is widely used to secure the system based on its complexity and infeasibility for easily decoding.
- We conducted tests with different deep learning models to see the performance of them, and if they can simply break the most general CAPTCHA.

Data
- We used a python script[2] to generate images of color captchas and controlled the size, rotation, warp and overlapping of the images.
- The dataset for each model consists of 12288 images with labels including 10240 training samples, 1024 validation samples and 1024 testing samples.
- Each image consists of 4 characters(10 digits, uppercase and lowercase letters).

Loss Equation
- We use Cross-Entropy as our loss function:
  \[ \sum (-y \cdot \log(p) - (1 - y) \cdot \log(1 - p)) \]

Model
- Segmentation: Identify Chars with Pixel Density

Discussion
- The performance of character classification based on segmentation is poor because of overlappings. Thus it's better to use end2end training in this kind of tasks.
- The usage of the grey scale image as the input highly increases the performance of our model because we don't require much color feature in this task.

Future Work
- Conduct transfer learning for other type of CAPTCHAs, and see how the transfer learning can support in character detection.
- Study the value of training models for nature character detection prepared with artificial occluded data.
- Implement some data preprocessing to remove the noise dots and curves from the image.

Reference
[1] captcha 0.3: https://pypi.org/project/captcha/
https://github.com/zhangy1234/breaking_captcha