



# Compare Different Model's Performance on Breaking CAPTCHA

Haotian Sun  
htsun@stanford.edu

Jiaying Li  
jiayingl@stanford.edu

Yutong Zhang  
yutong16@stanford.edu

## 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.



Figure 1. Sample CAPTCHA (Generated from captcha Python Package[1])

## 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:

$$\sum (-y * \log(p) - (1 - y) * \log(1 - p))$$

## Model

- Segmentation: Identify Chars with Pixel Density

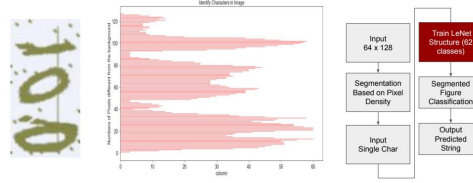


Figure 2. Segmentation Method

- End-to-End: VGG-16[3] Revised Structure
- 4x (2\*Conv2D+MaxPooling) + 2 x FC

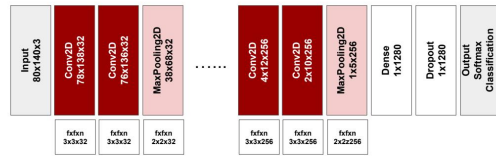


Figure 3. Revised VGG-16

## Results

	FC NN	LeNet + Segmentation	Simple CNN	VGG-16 Revised	ResNet50
Mini Batch Size	32	128	32	32	32
Dropout	0.7	1.0	0.25	0.25	0.7
Learning Rate	0.001	0.001	0.001	0.001	0.001
Optimizer	Adam	SGD	Adadelta	Adadelta	Adadelta
Epoch	60	50	60	60	60
Loss Function	CE	CE	CE	CE	CE
Test Accuracy	2.92%	< 1.00%	46.88%	85.16%	81.29%

Table 1. Performance from Multiple Model

## 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/>
- [2] GitHub Code: [https://github.com/haotiansun/keras\\_captcha](https://github.com/haotiansun/keras_captcha)  
[https://github.com/zhangyt1234/breaking\\_captcha](https://github.com/zhangyt1234/breaking_captcha)
- [3] Simonyan, K., Zisserman, A., (2015). Very Deep Convolutional Networks for Large-Scale Image Recognition. arXiv:1409.1556