Heaven's Light is Our Guide

Department of Computer Science and Engineering

Rajshahi University of Engineering and Technology

CAPTCHA Security Breaking System By Complex Character Recognition Using Deep Convolutional Neural Network

Presented By
Md. Adil Ali
Roll No: 143043
Dept. Of CSE, RUET

Supervised By
Julia Rahman
Assistant Professor
Dept. Of CSE, RUET

Outlines

- Objectives
- Related Works
- Dataset
- Dataset Pre-Processing
- Proposed Method
- Recognition By Deep Convolutional Neural Network
- Experimental Analysis
- Limitations
- Future work
- References

Overview of CAPTCHA

- CAPTCHA stands for "*completely automated public Turing test to tell computers and humans apart.*"
- A CAPTCHA is a program that protects websites against web robots by generating and grading tests that humans can pass but current computer programs can't.
- CAPTCHA can be different types like image, text, audio, video and puzzle.

Application of CAPTCHA

- Protecting Website Registration
- Online Polls
- Preventing Dictionary Attacks
- Protecting Email Addresses from Scrapers

Different types of CAPCHA

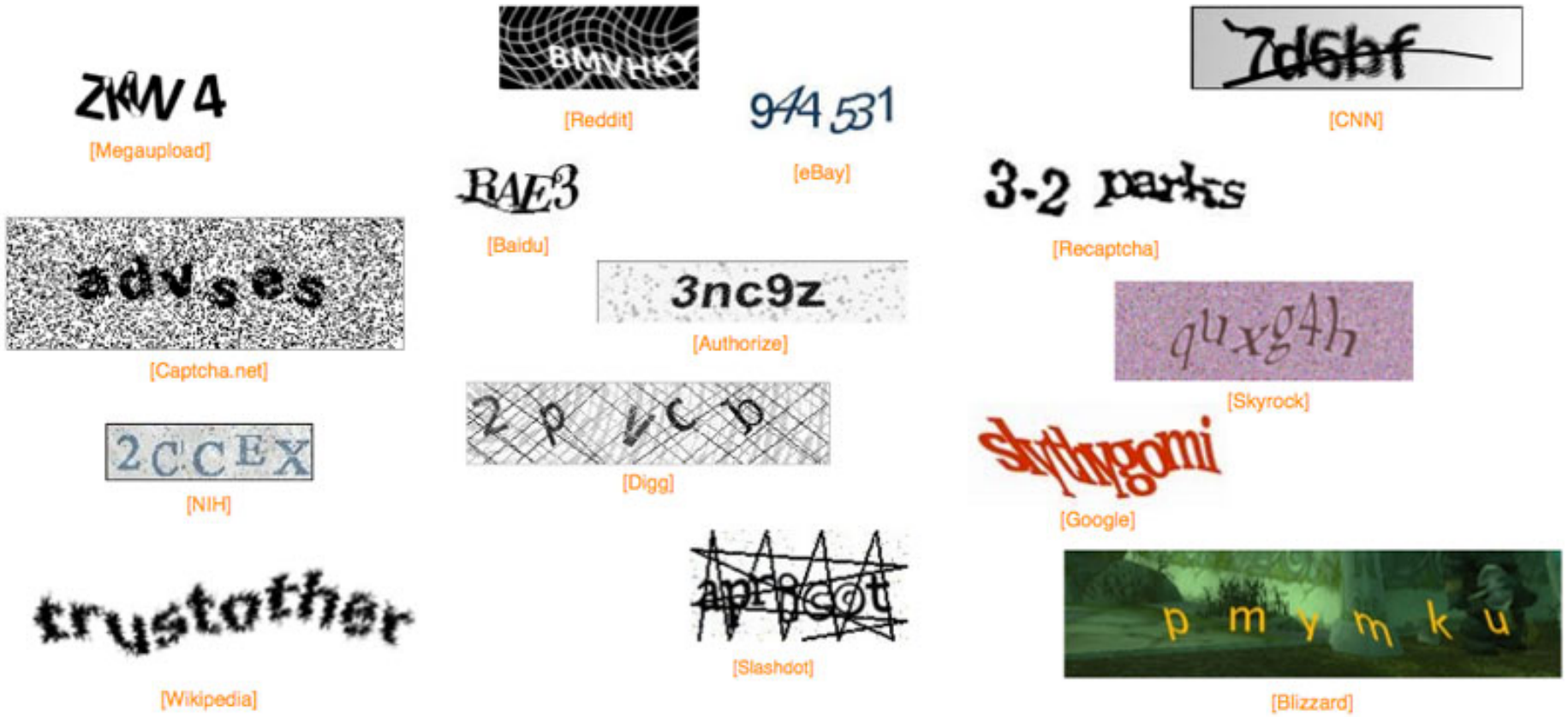


Fig 0. captcha of fifteen popular website [13]

Motivation

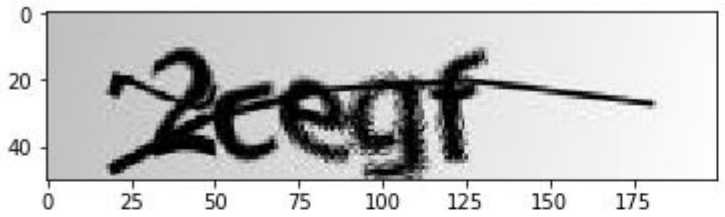
“ If you want to protect a system from intruder or bots at first you have to break like this system. Then you can take necessary steps to protect your system. ”

…. Khan md. Jahir raihan

Objectives

- CAPTCHA Security Breaking
- Complex Character Recognition
- Finding Weakness of Current CAPTCHA
- Making Stronger CAPTCHA System

My Objectives




```
]:
#Lets Predict By Model
print("Predicted Captcha =",predict('../input/captcha/capthaimage/capthaimages/a.png'))
```

```
Predicted Captcha = 2cegf
```

Fig 1: Demo Of CAPTCHA Security Breaking System

Related Works

- CAPTCHA: Using hard AI problems for security[1]
- Machine Learning System for breaking CAPTCHA[2]
- CAPTCHA as a web service [3]
- Multi-digit Number Recognition[4-5]
- KNN based CAPTCHA breaking [6]
- A low cost attack on Microsoft CAPTCHA [8]
- CAPTCHA security breaking [10]

Dataset

CAPTCHA Images Dataset [11] is used here for training and testing purpose. There are total 1070 images. There are total 36 symbols (26 English Letters+ 10 Digit)

Fig. 2. Sample Images of CAPTCHA Images Dataset

Dataset Pre Processing

- Images are converted to as gray scale image with one color channel.
- Scaled and Reshaped
- Labels are OneHotEncoded . Ex: 2 is [0,1,0,0…..0]
- Extracted Total Number of Symbols from Images.
- Total Number of Symbols are 36
- Extracted total number of character per images.

Proposed Method

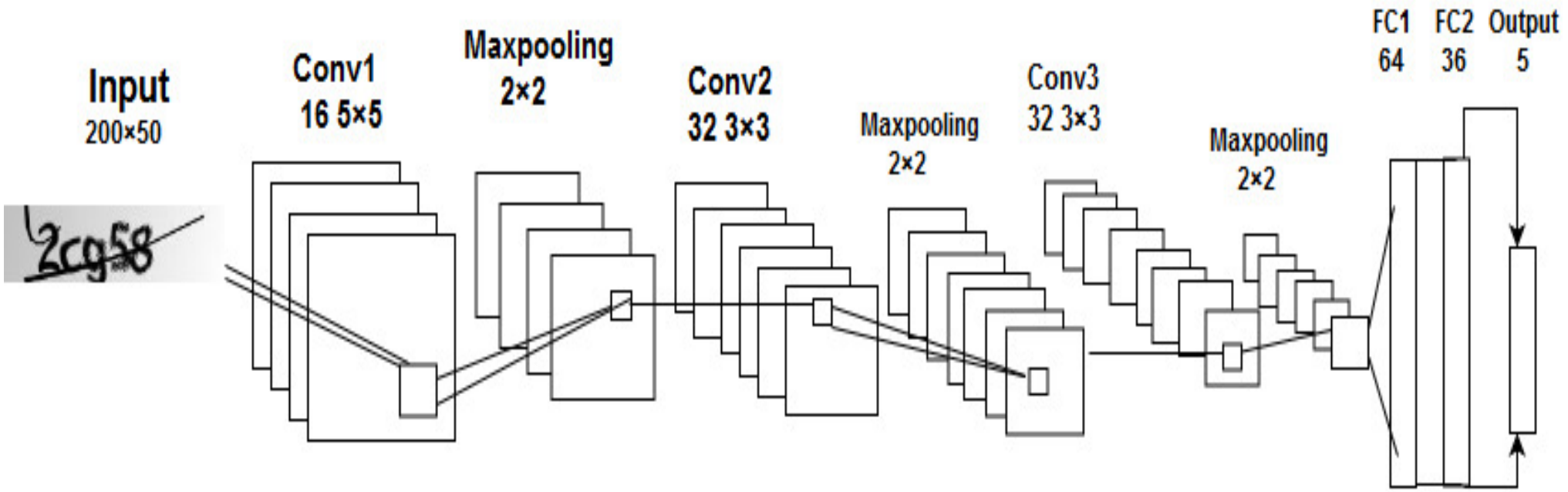


Fig.3. Proposed Architecture Model of CNN [12]

Deep Convolutional Neural Network

Architecture of this model is inspired by the architecture of previous researchers models [12]. But proposed model is different than inspired models and some changes are made for reducing training time. The proposed architecture is briefly described below.

- 3 convolutional layers with 3 layers 2×2 maxpooling layer and 2 fully connected dense layers.
- First layer has 16 filters and each filter size is 5×5
- The last two layers have 32 filters and each filter size is 3×3
- RELU (max(0,1)) is used as an activation function.
- The pool size of maxpooling layer is 2×2
- Dropout (0.2) is used to reduce the overfitting.

Deep Convolutional Neural Network

- Among the two fully connected layers, the first one has 64 filters and the last one has 36 filters for the 36 character.
- Flattened vector has 5 branches from it. Each branch will predict one letter.
- Sofmax function is used for the classification
- Adam optimizer is used for updating the weights.

Experimental Analysis

Experimental Environment

The experimental environment is configured with Intel Core i7 processor, Tesla k80 GPU and 16 GB of RAM. This environment has reduced our training time by keeping better performance of our model.

Training, Validation and Testing

The CAPTCHA dataset contains total of 1070 images. The dataset is divided into training, Validation and testing dataset keeping 776 (80%) images for training and 194 (20%) for validation. Rest of 100 images are for testing.

Experimental Analysis

Training Model Parameters

The training model of our architecture is dependent on some parameters. The parameters of the training model are given in Table I.

Parameters	Value
Learning rate	0.0001
Batch Size	32
Epoch	30

Table 1: Model Parameters

Experimental Analysis

Result Analysis

As the CAPTCHA is based on 5 characters, so in every label there are 5 sub label. By averaging the final result is shown below.

Label Position	Training Accuracy	Validation Accuracy	Testing Accuracy
1	98.07%	98.00%	99.33%
2	95.88%	94.33%	92.00%
3	94.33%	92.78%	85.18%
4	95.62%	89.18%	90.05%
5	97.42%	88.66%	86.07%
Full label	**96.26%**	**92.18%**	**90.32%**

Table 2: Result Analysis

Experimental Analysis

Table 3 shows the comparison of proposed method's result with previous researcher's result.

Proposed Method (Deep Learning)	Previous Method (Machine Learning) [10]
90.32%	67.42%

Table 3: Testing Accuracy Comparison with Previous Research

Limitations

- Small Number of Samples (1070 images)
- Same type of images
- Same type of pattern
- CAPTCHA is based on 5 Characters.

Future Work

- Experiment with Large number of samples
- Multiple Dataset
- Different type of CAPTCHA
- Extends of character per CAPTCHA.
- Comparison with other researchers result.

References

[1] L. Von Ahn, M. Blum, N. J. Hopper and J Langford, “CAPTCHA: Using hard AI problems for security,” *International Conference on the Theory and Applications of Cryptographic Techniques*, Springer, Berlin, Heidelberg, 2003, pp. 294-311.

[2] K. Chellapilla and P. Y. Simard, "Using machine learning to break visual human interaction proofs," *Advances in neural information processing systems*, 2005, pp. 265-272.

[3] T. Converse, “CAPTCHA Generation as a Web Service.” *Proc*. *Human Interactive Proofs*, Springer, Berlin, Heidelberg, 2005, pp. 82-96.

[4] I. J. Goodfellow, Y. Bulatov, J. Ibarz, S. Arnoud and V. Shet, “Multi-digit Number Recognition from Street View Imagery using Deep Convolutional Neural Networks,” *Computer Science*, 2013.

[5] M. Jaderberg, A. Vedaldi, and A. Zisserman, “Deep features for text spotting,” *European conference on computer vision*, Springer, Cham, 2014, pp. 512-528.

[6] Y. Wang, Y. Q. Xu, Y. B. Peng, “KNN-based Verification Code Recognition Technology

References

[7] P. Y. Simard, D. Steinkraus and J. C. Platt, “Best practices for convolutional neural networks applied to visual document analysis,” *International Conference on Document Analysis and Recognition IEEE Computer Society*, Vol. 3, 2003, pp. 958-962.

[8] J. Yan, A. S. E. Ahmad, “A low-cost attack on a Microsoft captcha,” *ACM Conference on Computer and Communications Security*, CCS 2008,

[9] G. Mori and J. Malik, “Recognizing objects in adversarial clutter: Breaking a visual CAPTCHA,” *Computer Vision and Pattern Recognition*, 2003. *Proc*. *IEEE Computer Society Conference*, Vol. 1, IEEE, 2003, pp.

[10] Wilhelmy, Rodrigo & Rosas, Horacio. (2012). A Comparison of Supervised Learning Algorithms to Solve CAPTCHAs.

[11] CAPTCHA Dataset [Last Accessed:February 2019] https://www.kaggle.com/fournierp/captcha-version-2-images

[12] A. Shawon, M. Jamil-Ur Rahman, F. Mahmud and M. M. Arefin Zaman, "Bangla Handwritten Digit Recognition Using Deep CNN for Large and Unbiased Dataset," *2018 International Conference on Bangla Speech and Language Processing (ICBSLP)*, Sylhet, 2018, pp. 1-6.
doi: 10.1109/ICBSLP.2018.8554900

[13] https://www.helpnetsecurity.com/2011/11/01/how-to-create-effective-captchas/

Thank You