ICAI 2023
12th International Conference on Applied Informatics
Eger, Hungary, 2023

CAPTCHA recognition using machine learning algorithms with different techniques

Ádám Kovács[a], **Tibor Tajti**[b]

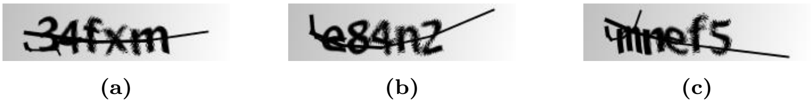
[a]Eszterházy Károly Catholic University
kovacs2.adam@uni-eszterhazy.hu

[b]Eszterházy Károly Catholic University
tajti.tibor@uni-eszterhazy.hu

Abstract

CAPTCHA, short for Completely Automated Public Turing test to tell Computers and Humans Apart, is a widely used security measure to differentiate between human and machine users [7]. However, with the advancement of artificial intelligence techniques, traditional CAPTCHAs can be easily bypassed by automated systems. In this abstract, we propose machine learning models for CAPTCHA recognition and discuss the techniques of hyperparameter tuning, early stopping, and ensemble methods to improve the performance of the model [1, 3].

First, the dataset of CAPTCHAs and their corresponding labels were collected, which consists of text-based CAPTCHA codes, each containing five alphanumeric characters [6]. Then the data is preprocessed, including image resizing and character extracting from the name of the images.



(a) **(b)** **(c)**

Figure 1. Text-based CAPTCHA patterns

Figure 1 depicts a variety of text-based CAPTCHAs from the dataset, each of which has been subjected to various forms of noise and distortion. These modifications serve to make the CAPTCHAs more difficult for automated systems to interpret, thereby increasing the security of the system they are protecting.

Next, different convolutional neural networks (CNN) and recurrent neural networks (RNN) are trained on the dataset [4]. CNNs are particularly suitable for image recognition tasks, as they can extract features from images and learn the patterns in the data. Besides that there are various methods have been proposed for circumventing text-based CAPTCHAs, one such example being the DFCR (DenseNet for CAPTCHA recognition) approach, which utilizes DenseNets as the underlying architecture [5].

To improve the performance of the models, parameter tuning was performed using grid search. This involves varying the hyperparameters of the model, such as the number of layers, the learning rate, and the dropout rate, and evaluating the model's performance on a validation set. At the end of the process, the set of hyperparameters that resulted in the best performance was selected.

To prevent overfitting early stopping was implemented. It occurs when the model becomes too complex and starts to fit the noise in the training data, rather than the underlying patterns. Early stopping involves monitoring the performance of the model on a validation set and stopping the training when the performance starts to deteriorate.

In addition to the above techniques, the application of ensemble methods was also used to further improve the performance of the CAPTCHA recognition models. There are many popular ensemble methods, like bagging and voting [2]. They involve combining the outcomes of multiple or the same models to make a final prediction. The idea behind this approach is that various types of models have different strengths and weaknesses and by combining them, their strengths can be leveraged to compensate for their weaknesses. These methods are commonly used in problems such as classification and regression, and they have been shown to improve the performance of machine learning models in many applications.

Finally, the performance of the models was evaluated on the test set, the accuracies were reported, and the results were visualized, providing insights on how to improve the models' performance.

In conclusion, different machine learning models were created for text CAPTCHA recognition and the techniques of parameter tuning, early stopping, and ensemble methods were discussed to improve the performance of the models. It is important to note, that these techniques can be applied to other image recognition tasks as well. However, this research is still an ongoing field and there is still room for improvement in terms of performance and robustness. As technology continues to evolve, it is crucial to continuously monitor and update CAPTCHA systems to ensure they remain effective in protecting online services from automated bots and malicious actors.

References

[1] T. G. Dietterich: *Ensemble Methods in Machine Learning*, in: Multiple Classifier Systems, Berlin, Heidelberg: Springer Berlin Heidelberg, 2000, pp. 1–15, isbn: 978-3-540-45014-6, doi: https://doi.org/10.1007/3-540-45014-9_1.

[2] L. Kabari, U. Onwuka: *Comparison of Bagging and Voting Ensemble Machine Learning Algorithm as a Classifier*, International Journal of Computer Science and Software Engineering 9 (Mar. 2019), pp. 19–23.

[3] L. Prechelt: *Early Stopping - But When?*, in: Neural Networks: Tricks of the Trade, ed. by G. B. Orr, K.-R. Müller, Berlin, Heidelberg: Springer Berlin Heidelberg, 1998, pp. 55–69, isbn: 978-3-540-49430-0, doi: https://doi.org/10.1007/3-540-49430-8_3.

[4] Y. Shu, Y. Xu: *End-to-End Captcha Recognition Using Deep CNN-RNN Network*, in: 2019 IEEE 3rd Advanced Information Management, Communicates, Electronic and Automation Control Conference (IMCEC), 2019, pp. 54–58, doi: https://doi.org/10.1109/IMCEC46724.2019.8983895.

[5] J. Wang, J. Qin, X. Xiang, Y. Tan, N. Pan: *CAPTCHA recognition based on deep convolutional neural network*, Mathematical Biosciences and Engineering 16.5 (2019), pp. 5851–5861, issn: 1551-0018, doi: 10.3934/mbe.2019292.

[6] R. Wilhelmy, H. Rosas: *captcha dataset*, July 2013.

[7] Y. Zhang, H. Gao, G. Pei, S. Luo, G. Chang, N. Cheng: *A Survey of Research on CAPTCHA Designing and Breaking Techniques*, in: 2019 18th IEEE International Conference On Trust, Security And Privacy In Computing And Communications/13th IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), 2019, pp. 75–84, doi: https://doi.org/10.1109/TrustCom/BigDataSE.2019.00020.