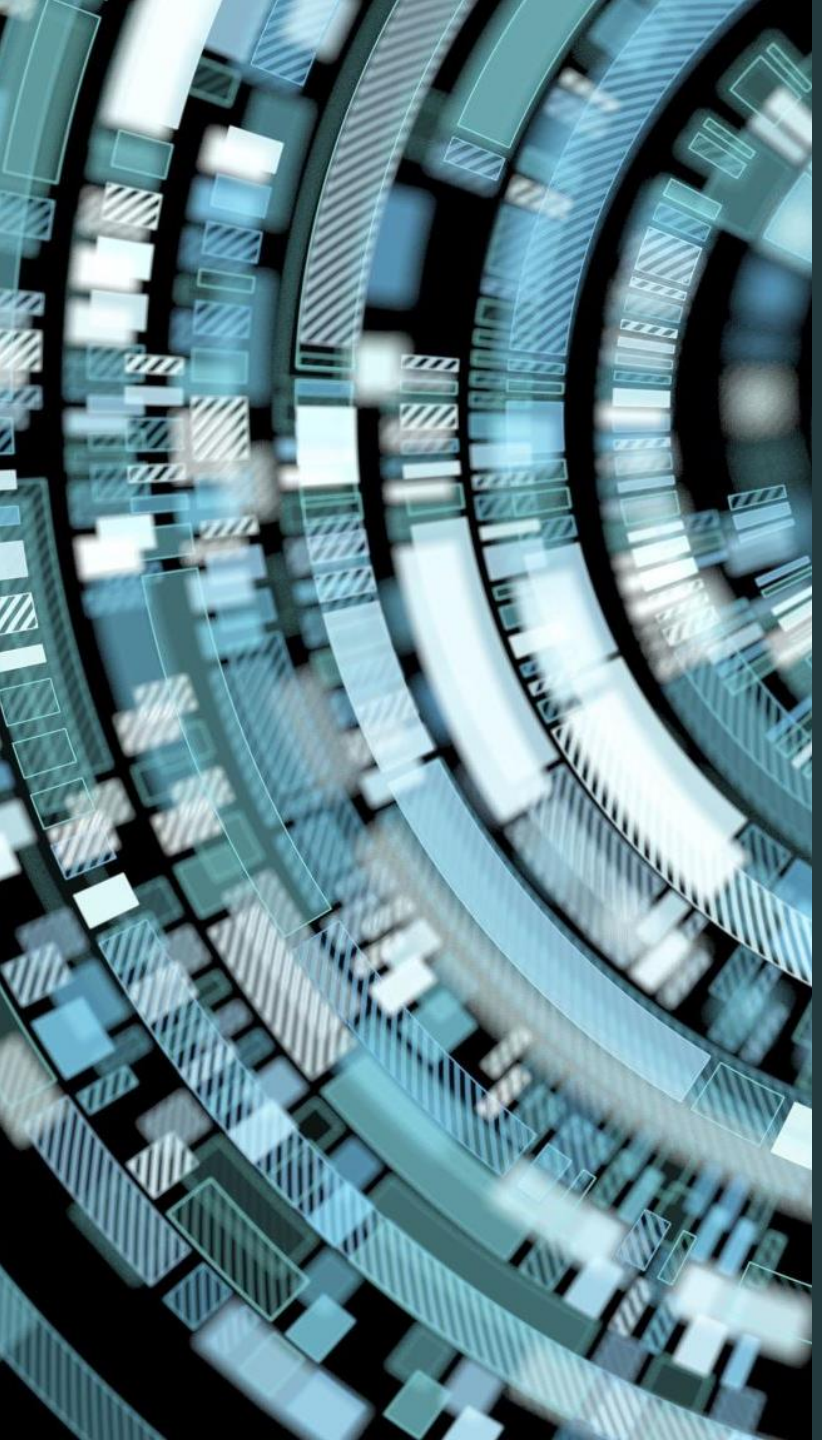


CSL2010 INTRODUCTION TO ML COURSE PROJECT

Title - Using Machine Learning to break Visual Human Interactive Proofs (HIPs)

Name – Tejas Manoj Jamdade

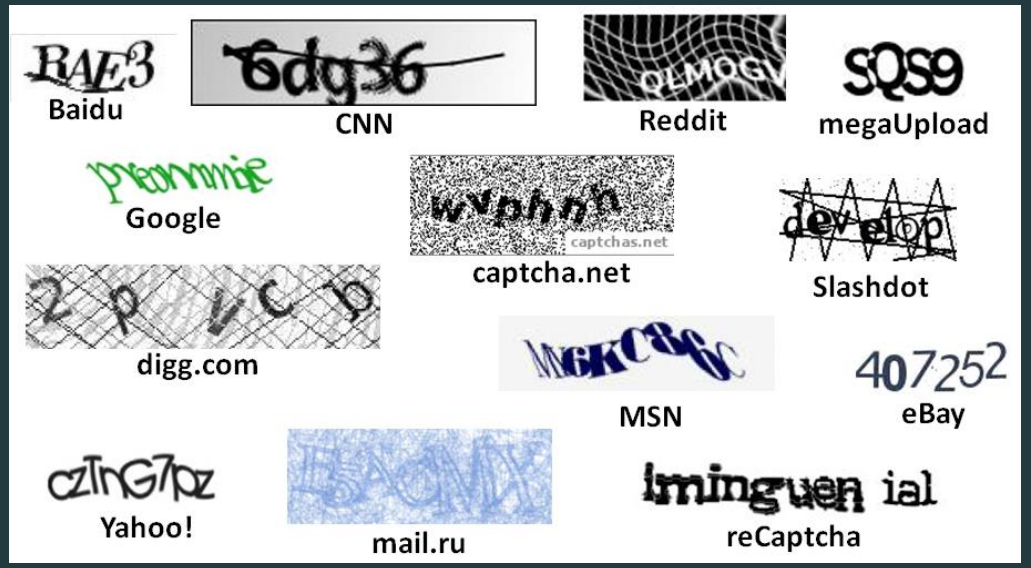
Roll No – B20MT049

INTRODUCTION

- Machine learning is often used to automatically solve human tasks. In this paper, the author uses it to differentiate between a human and a computer.
- Work on distinguishing computers from humans traces back to the original Turing Test which asks that a human distinguish between another human and a machine by asking questions of both.

HUMAN INTERACTIVE PROOFS (HIPS)

- Human Interactive Proofs (HIPs) or Completely Automated Public Turing Tests to Tell Computers and Humans Apart (CAPTCHAs) are tests that enable the construction of automatic filters that can be used to prevent automated scripts from utilizing services intended for humans.
- Harder HIPs are built using the combination of recognition and segmentation tasks. Hence segmentation is the most effective way to confuse the machine learning algorithms.



DATASET

- For testing the algorithm they have used the MNIST dataset.
- 2500 HIPs were hand labeled and used as - (a) recognition [1600 for training, 200 for validation, and 200 for testing], and (b) segmentation [500 for testing segmentation]

USING MACHINE LEARNING TO BREAK HIPS

- Our generic method for breaking all the HIPs is to write a custom algorithm to locate the characters and then use machine learning for recognition.
- Surprisingly, segmentation, or finding the characters, is simple for many HIPs; which makes the process of breaking the HIP particularly easy.

LESSONS LEARNED FROM BREAKING HIPS

For successful segmentation, our system must learn to identify which patterns are valid among the set of all the possible valid and non-valid patterns.

Harder HIPs can be built by making the segmentation difficult. The idea is that the additional arcs are themselves good candidates for false characters.

CONCLUSION

- *Segmentation plays a major role in building better/harder HIPs.*
- Decomposing the process into recognition and segmentation simplifies the analysis.
- Recognition on even unprocessed images can be done automatically using neural networks

BIBLIOGRAPHY

[1] Baird HS (1992), "Anatomy of a versatile page reader," IEEE Pro., v.80, pp. 1059-1065.
[2] Turing AM (1950), "Computing Machinery and Intelligence," Mind, 59:236, pp. 433-460.
[3] First Workshop on Human Interactive Proofs, Palo Alto, CA, January 2002.
[4] Von Ahn L, Blum M, and Langford J, The Captcha Project. http://www.captcha.net
[5] Baird HS and Popat K (2002) "Human Interactive Proofs and Document Image Analysis," Proc. IAPR 2002 Workshop on Document Analysis Systerms, Princeton, NJ.
[6] Simard PY, Steinkraus D, and Platt J, (2003) "Best Practice for Convolutional Neural Networks Applied to Visual Document Analysis," in International Conference on Document Analysis and Recognition (ICDAR), pp. 958-962, IEEE Computer Society, Los Alamitos.
[7] Mori G, Malik J (2003), "Recognizing Objects in Adversarial Clutter: Breaking a Visual CAPTCHA," Proc. of the Computer Vision and Pattern Recognition (CVPR) Conference, IEEE Computer Society, vol.1, pages:I-134 - I-141, June 18-20, 2003
[8] Chew, M. and Baird, H. S. (2003), "BaffleText: a Human Interactive Proof," Proc., 10th IS&T/SPIE Document Recognition & Retrieval Conf., Santa Clara, CA, Jan. 22.
[9] LeCun Y, Bottou L, Bengio Y, and Haffner P, "Gradient-based learning applied to document recognition,' Proceedings of the IEEE, Nov. 1998.