Two Deep Learning Papers Robustness and Security in ML Systems, Spring 2021

Jonathan Soma

January 19, 2021

Handwritten Digit Recognition with a Back-Propagation Network, 1990

Y. Le Cun, B. Boser, J. S. Denker, D. Henderson, R. E. Howard, W. Hubbard, and L. D. Jackel

a.k.a. LeCun90c

Yann LeCun

Yann LeCun on Wikipedia

Figure 1: Yann LeCun on Wikipedia

Chief AI Scientist (and several other titles) at Facebook, "founding father of convolutional nets."

All kinds of badly programmed computers thought that "Le" was my middle name. Even the science citation index knew me as "Y. L. Cun", which is one of the reasons I now spell my name "LeCun". From Yann's Fun Stuff page Also: Falsehoods Programmers Believe About Names

The Problem

How to turn handwritten ZIP codes from envelopes into numbers Examples of original zipcodes from the testing set

Figure 2: Examples of original zipcodes from the testing set