

Writeup for Project 1b

What were some common mistakes in labeling, if any in your process?

One dataset (1619be3e) involved complicated layouts across five settings with many objects, with a digit pattern eventually emerging. In the many ambiguous cases in this dataset, I needed to reason about the human decisionmaking process that would have gone into constructing the image. For example, if I thought the shape in an image could correspond to two possible digits, I thought about what choices the dataset creator would have made in both cases, and in which case the choices about the overall structure of the image I had in front of me would make sense.

Dataset 3a6ba065 had some settings which were rather low-contrast – I feel confident in all my labels but needed to squint a little for a few images.

Dataset 35afbc6 adopted an approach of destroying initially clear images with digital editing. As such, using color, it was fairly easy as a human to not only label the image correctly but discern the original structure, and since the perturbations were applied locally everywhere, the global structure of the digit was clearly retained. I did not have any issues labeling this dataset.

What are some strengths and weaknesses of this dataset? What conditions do you think a model would struggle with?

Dataset 1619be3e contains diverse settings with poor local structure in the digits. This may require models to take into account the global structure of the images to accurately label them, which I found necessary when labeling them myself. A model which is able to learn this kind of feature extraction will likely be robust to future adversarial images and will likely demonstrate strong generalization capability. However, I am pessimistic about a model without extremely strong feature representation and internal ‘reasoning’ abilities being able to learn anything meaningful from, or well on, this dataset.

Dataset 3a6ba065 has many images which rely on distinguishing between colors and ignoring background noise, which may be difficult for models to work with. I think taking into account all available color channels, and using filters which amplify contrast differences to detect edges, will be extremely important for the performance of the models.

Dataset 35afbc6 has very noisy local structure so a model should be able to take into account global structure to capture features in it. There are also jarring color discontinuities which may damage assumptions about edge detection.

Any extra comments?

The approaches displayed a lot of diversity and creativity, with settings spanning from arranging humans to complex digital edits. I am extremely curious to see

what kinds of kernels a model fit on this combined dataset learns, since extremely robust generalization will be required during training.