Convolutional Siamese Networks for Authorship Verification

Lawrence Hessburg, Payoj Jain, Poorwa Hirve, Prathyusha Gayam

University of Colorado, Boulder

Aim of the Project

The aim of our project is to design a Siamese Convolutional Network (Siamese CNN) in order to solve the Authorship Verification problem. We have designed a deep **ResnetSiamese** network and performed the following analysis:

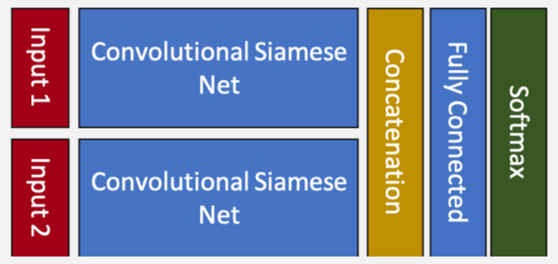
- Evaluated networks performance using accuracy, false positive rate and false negative rate metric
- Tested the model against fake images generated using a Cycle-GAN model

Background

Authorship verification problem is defined as differentiating between two pieces of handwriting and determining whether they belong to the same author. Most studies have been done for signature verification, which led to the development of Siamese CNN in 1993. Our project extends to the authorship verification problem, which also fits well with the Siamese CNN network.

Basic Network Structure

A basic Siamese CNN network has the following structure:



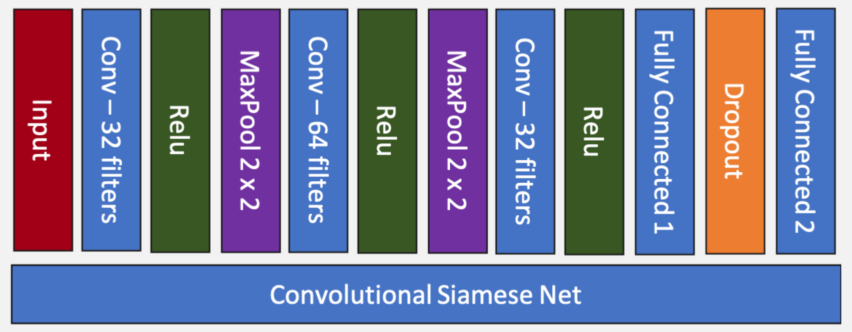
Two inputs images (1, 2) are fed through an identical network. The output encodings (a, b) from these are concatenated to get the following vector:

$$v = [\quad a \quad b \quad (a-b)^2 \quad a \odot b \quad]$$

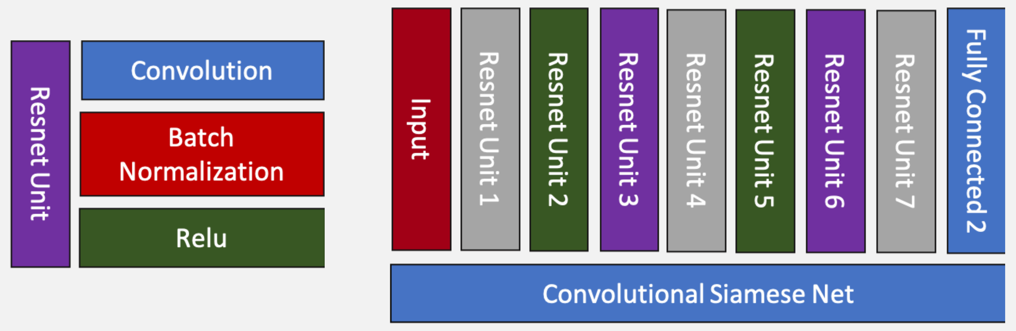
This vector is then finally fed into a fully connected layer to output the class scores.

Implemented Network Structures

- Simple Baseline network



- Resnet Siamese - a deep network



Methodology

1. Data pre processing - We used the **IAM Handwriting Database** to train our ResnetSiamese and pre-process the data to obtain images from authors.
2. Generate train and validation data files - Using this data, we generated image pairs to train and test our network with.
3. Training - We feed the train image pairs on both the networks
4. Testing - Lastly, our network models are evaluated against the (real,real) and (real,fake) image pairs

Results

Baseline

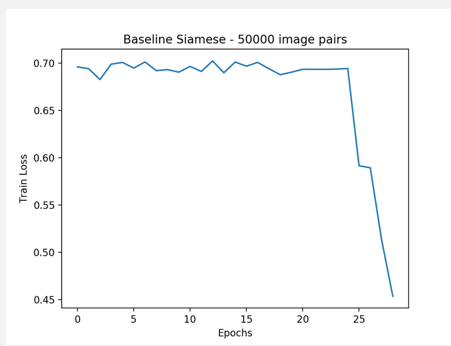


Figure: Training Loss

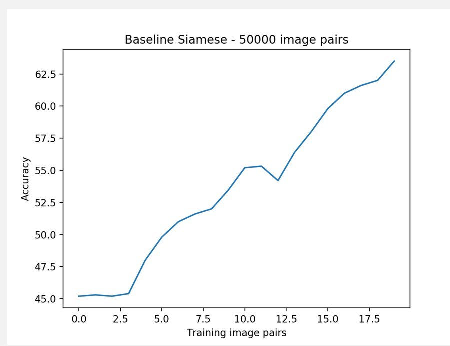


Figure: Test Accuracy

Resnet Siamese

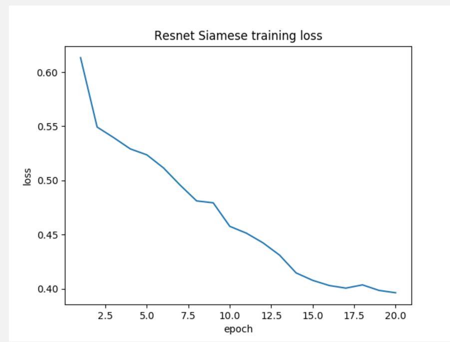


Figure: Training Loss

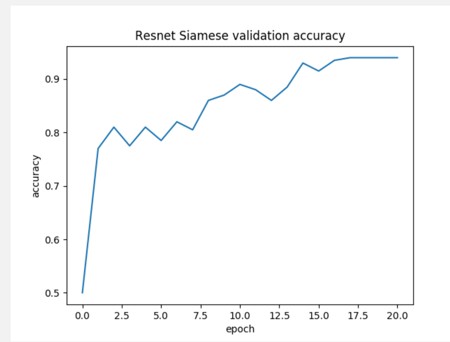


Figure: Test Accuracy

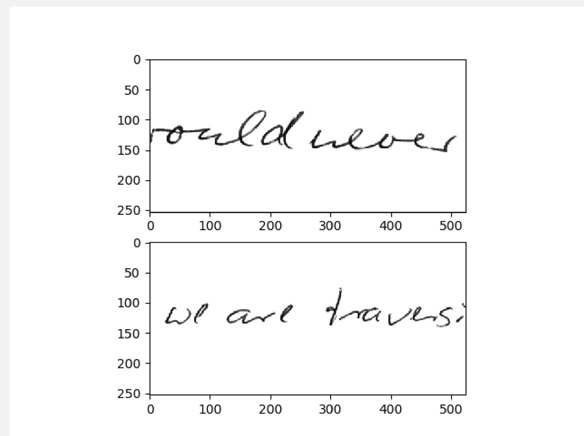
ResnetSiamese Evaluation

As seen in the previous graphs, ResnetSiamese performs better in terms of accuracy and loss as compared to the baseline.

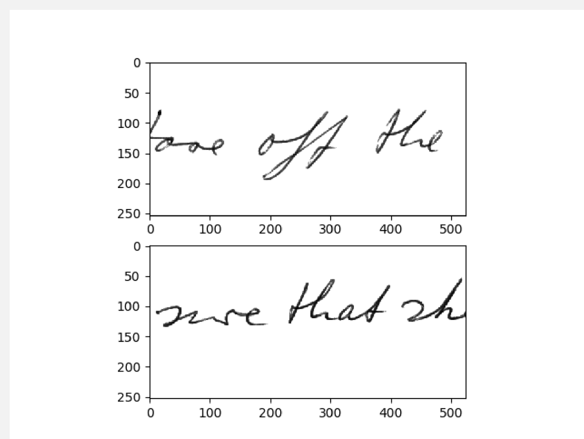
Train Size	Val Size	Val Acc	FP rate	FN rate
80	2000	64.6%	23.65%	11.75%
800	2000	74.75%	15.95%	9.3%
8000	2000	87.1%	6.55%	6.35%
40000	2000	93.7%	4.15%	2.15%

Examples of false positive and false negative from the best model:

1. False Positive:



2. False Negative:



GAN Results

We also trained a Cycle-GAN model in order to see if our best model would be able to detect fake generated or "forged" examples. We got the following results:

Train Size	Val Size	Val Acc	FP rate	FN rate
35	60	46.87%	6.25%	46.77%
70	60	53.33%	13.33%	33.3%

Challenges/Difficulties

- Modeling the Siamese CNN networks in pytorch
- Hyper parameter and optimizer tuning
- Spent a significant amount of time figuring out the working of google cloud for GPU access
- Insufficient documentation of data formatting in our references

References

[1] William Weidong Du, Michael Fang, and Ming Shen, Siamese convolutional neural networks for authorship verification, 2017.

[2] Jane Bromley, Isabelle Guyon, Yann Lecun, Eduard Scklnger, and RoopakShah, Signature verification using a 'siamese' time delay neural network, 1994.

[3] U.V. Marti and H. Bunke, The IAM-database: An english sentence database for offline handwriting recognition, *International Journal on Document Analysis and Recognition*, 5(1):39-46, 2002.

[4] `https://github.com/junyanz/pytorch-CycleGAN-and-pix2pix.git`

GitHub Repository

`https://github.com/phirwe/CSCI5922-Siamese-CNN-For-Authorship-Verification.git`