Munish Persaud

Mentor: Dr. Amrit Singh Bedi

Week 3

UCF CRCV REU 2025

Introduction

Education

University of Central Florida

Rising senior majoring in Computer Science and Biomedical Sciences with a minor in Nonprofit Management

Skills

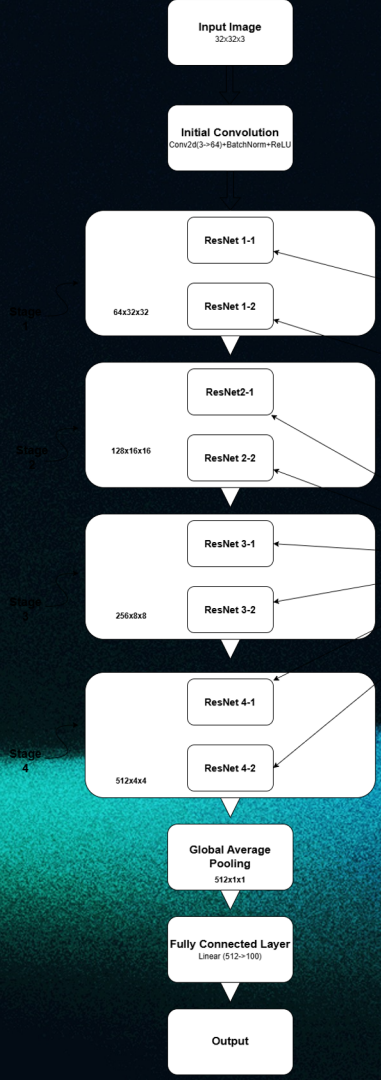
- PyTorch, TensorFlow
- C, C++
- SQL
- Java

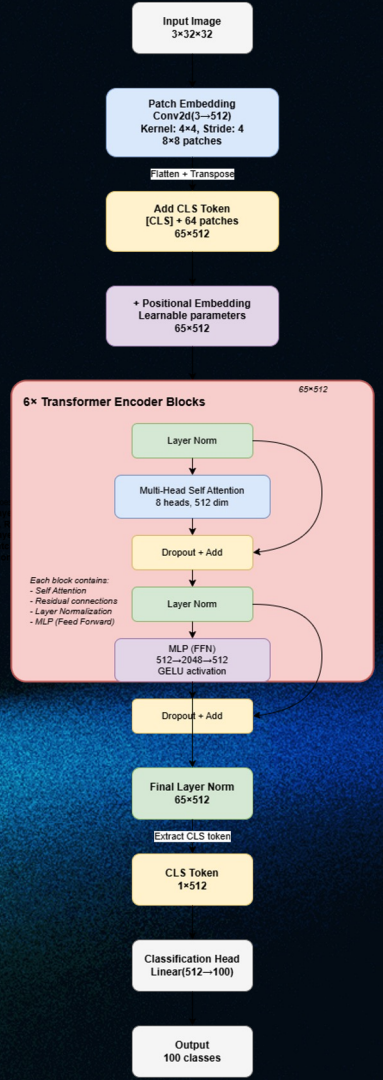
Previous Research

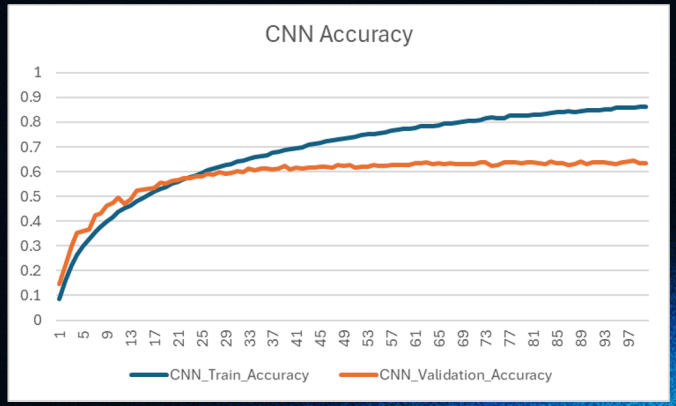
- Segmentation of cardiac cells to measure ejection fraction.
- Genomic research for the creation of a novel genetic therapy with CRISPR.

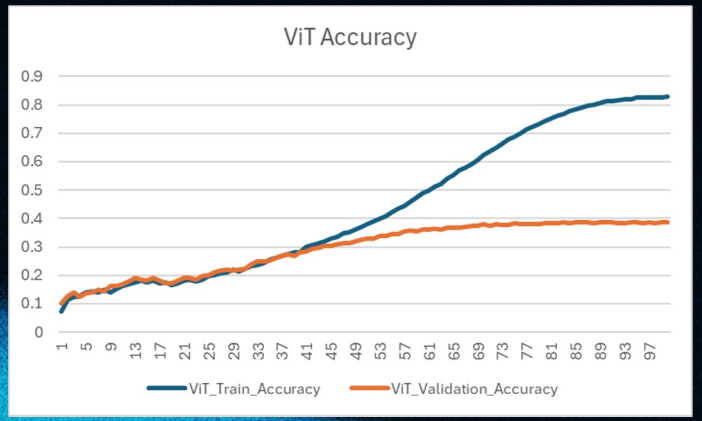
Assignment 1

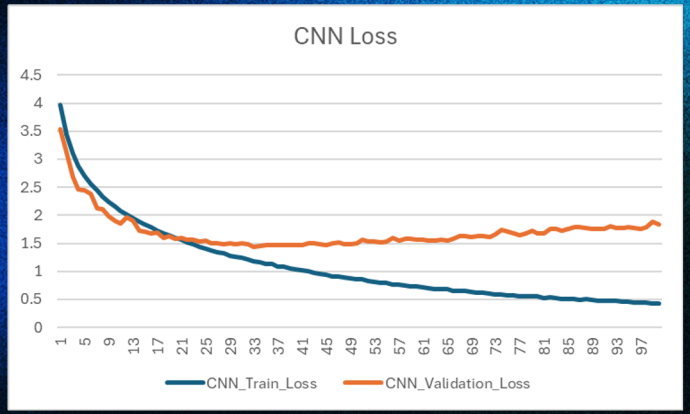
- Classification task from CIFAR-100 dataset.
- Built a ViT from scratch.
- Used a custom form of ResNet-18 to build a CNN from scratch.
- Both in PyTorch
- Both trained over 100 epochs.
- CNN architecture:
- ViT architecture:

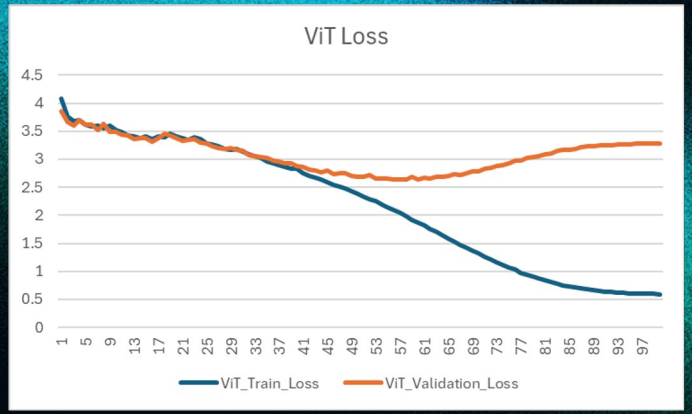


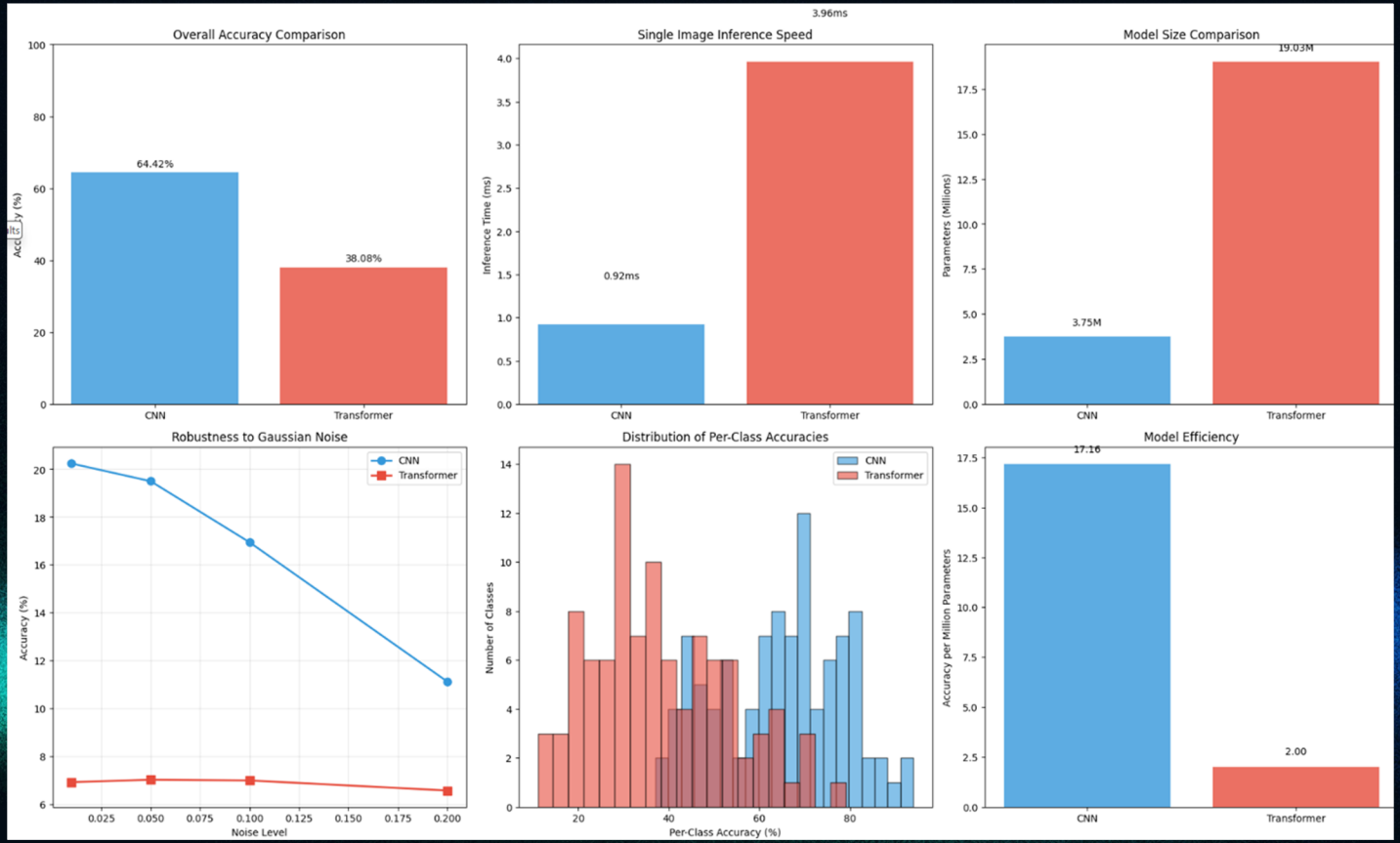



CNN Accuracy
CNN_Train_Accuracy
CNN_Validation_Accuracy


ViT Accuracy
ViT_Train_Accuracy
ViT_Validation_Accuracy


CNN Loss
CNN_Train_Loss
CNN_Validation_Loss


ViT Loss
ViT_Train_Loss
ViT_Validation_Loss


3.96ms
Overall Accuracy Comparison
Accuracy (%)
64.42%
38.08%
CNN
Transformer
Single Image Inference Speed
Inference Time (ms)
0.92ms
CNN
Transformer
Model Size Comparison
Parameters (Millions)
19.03M
3.75M
CNN
Transformer
Robustness to Gaussian Noise
Accuracy (%)
Noise Level
CNN
Transformer
Distribution of Per-Class Accuracies
Number of Classes
Per-Class Accuracy (%)
CNN
Transformer
Model Efficiency
Accuracy per Million Parameters
17.16
2.00
CNN
Transformer

Project Vision

Utilize Evo2

A generative model from Arc Institute that takes DNA and gives functional 3D protein structures.

Explore and test methods of jailbreaking and defending

One current method, “Genebreaker”, in pre-print that provided evidence jailbreaking Evo2 is possible.

Raise call to action for better safety parameters

Consequences are dangerous given the right set of conditions ie. the pre-print produces two novel SARS-CoV-2 spike protein variants

Current Progress

Literature Review

Evo2 sister papers, Genebreaker paper, papers on other models for scoring and guiding generation.

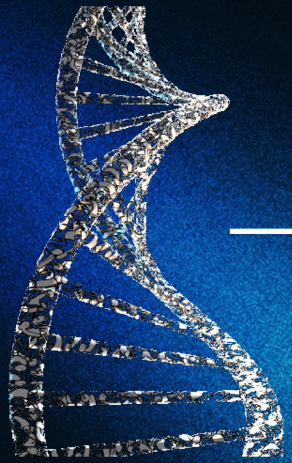
Model import attempt

No current access to H100's. That is a requirement due to FP8 format the model was developed on. A100's on Colab are in FP16 format. Emulation attempt failed. No access to 4000 series or 5000 series consumer grade GPU's either.

Data Evaluation

Training and test data is open source. I have been exploring to find gaps in training data and homologs to exploit.

Upcoming Deliverables



June 9th

Outside evaluation models chosen, scoring function in progress, and data collection.

June 11th

Model running on Newton

June 11th-15th

Pre-print experiment results reproduced

June 11th-15th

Methods for experiments and evaluation determined. Start experimenting.

Sources

- [Online Video]. [Online]. Available:(https://www.youtube.com/watch?v=7o1jpvapaT0).
- G. Brixi *et al.*, "Genome modeling and design across all domains of life with Evo 2," *bioRxiv*, 2025.02.18.638918v1, Feb. 2025. [Online]. Available: https://www.biorxiv.org/content/10.1101/2025.02.18.638918v1. (Original announcement: ArcInstitute, "Genome modeling and design across all domains of life with Evo 2," Feb. 19, 2025. [Online]. Available: https://arcinstitute.org/manuscripts/Evo2).
- ArcInstitute, "evo2: Genome modeling and design across all domains of life," GitHub repository. [Online]. Available: https://github.com/ArcInstitute/evo2.
- P. Notin *et al.*, "ProteinGym: Large-Scale Benchmarks for Protein Design and Fitness Prediction," *bioRxiv*, 2023.12.07.570727, Dec. 2023, PMID: 38106144. [Online]. Available: https://www.biorxiv.org/content/10.1101/2023.12.07.570727. (Also accessible via https://pubmed.ncbi.nlm.nih.gov/38106144/).
- Q. Zhang *et al.*, "Scientific Large Language Models: A Survey on Biological & Chemical Domains," arXiv:2401.14656v2 [cs.CL], Jul. 2024. [Online]. Available: https://arxiv.org/abs/2401.14656, doi: 10.48550/arXiv.2401.14656.
- S. K. Pentyala *et al.*, "PAFT: A Parallel Training Paradigm for Effective LLM Fine-Tuning," arXiv:2406.18045v1 [cs.CL], Jun. 2024. [Online]. Available: https://arxiv.org/html/2406.18045v1.
- P. Kashyap, "Understanding SGD with Momentum in Deep Learning: A Beginner-Friendly Guide," *Medium*. [Online]. Available: https://medium.com/@piyushkashyap045/understanding-sgd-with-momentum-in-deep-learning-a-beginner-friendly-guide-0252ede605b4. (Publication date not available in provided materials).
- D. Luo, J. Zhou, L. Xu, S. Yuan, and X. Lin, "DynamicDTA: Drug-Target Binding Affinity Prediction Using Dynamic Descriptors and Graph Representation," arXiv:2505.11529v1, May 2025, accepted for publication in *Interdisciplinary Sciences: Computational Life Sciences*. [Online]. Available: https://arxiv.org/abs/2505.11529, doi: 10.48550/arXiv.2505.11529.
- S. Ishida and K. Terayama, "Large language models open new way of AI-assisted molecule design for chemists," *J. Cheminform.*, vol. 17, no. 1, Art. no. 36, Mar. 2025, doi: 10.1186/s13321-025-00984-8.
- Z. Zhang, Z. Zhou, R. Jin, L. Cong, and M. Wang, "GeneBreaker: Jailbreak Attacks against DNA Language Models with Pathogenicity Guidance," arXiv:2505.23839v1, May 2025. [Online]. Available: https://arxiv.org/abs/2505.23839, doi: 10.48550/arXiv.2505.23839.

Questions?