CYBR 560 Capstone Prospectus

Jeet Kumar

jk32@hood.edu

Fall 2024

1. Capstone Project Title: Comparative Analysis of ResNet RS and EfficientNetV2 Convolutional Neural Networks in Regards to Deepfake Detection
2. Research Problem: In my capstone project, my main goal is to compare the two latest models of the two main libraries of Convolutional Neural Networks (CNNs) that are ResNet and EfficientNet. I will be providing an unfiltered and unbiased comparison of these two models to communicate the similarities and differences. This will help professionals in the industry learn and understand which library is more efficient, quicker, less resource-intensive, etc. It will also help them understand which model is the better use case in different circumstances.
3. Assumptions: For this project, I will be assuming that ResNet RS and EfficientNet V2 are the most current versions of each their respective libraries and they will be comparable in terms of efficiency, accuracy, and other parameters I will be using to assess the models.

I will also be assuming that these two libraries are closely related in terms of architecture and scaling. This will need to be researched further and could also provide some interesting results based on the methodology.

For the experiment, I will be using the FaceForensics++ database in order to train the two CNNs and I will be assuming that this is a reliable and comprehensive collection of images that will perform adequately with both models and will provide an accurate showcase of their capabilities and shortcomings.

1. Literature Review: According to the research related to ResNet, it was formulated as a way of training networks which is considered to be deeper than any neural networks used previously. By establishing more layers in a residual net, there is a decrease in error and significant increase in object detection. This is a convolutional neural network was given the name “ResNet”[1]. As the library and architecture evolved, the methodology changed and was restructured into a new family, ResNet-RS which is proven to be 1.7x-2.7x faster than EfficientNets while achieving similar accuracies [2].

EfficientNet was created as a scaling tool to balance network depth, width and resolution and is considered to be more accurate and efficient than any previous ConvNets [3]. EfficientNetV2 is considered to be more efficient than the previous model by using a unique neural architecture search and scaling technique which will provide an interesting comparison to ResNet-RS[4].

1. Research Questions: How will I assess the two convolutional neural networks? How can I accurately measure their efficacy? How can I showcase their differences in performance?
2. Research Plan: For this thesis, I will be assessing both the EfficientNet V2 and ResNet RS in terms of performance. I will be measuring them specifically with metrics like accuracy, speed, and computational efficiency. In order to measure them accurately, I will need to understand and explain briefly the differences between the two architectures and how these differences will affect the results of the experiment. Using this I will also be able to answer and alleviate any concerns related to their computational efficiency by monitoring their performance throughout the detection process. Providing evidence with physical data and charts will assist with this and provide an accurate analysis of their performance and build a comprehensive comparison of the two models.
3. Expected Outcome: At the end of my thesis, I will be providing an unbiased examination of the performance of EfficientNet V2 and ResNet RS as they detect and analyze deepfakes.
4. Project Plan: For this project I will create an experiment that will compare the efficacy of both EfficientNetV2 and ResNet RS. Both models can be found in Github or in external libraries. In order to setup the experiment, I will need to have the proper hardware to handle the computations that will be done by the models. I will need to install coding software like Python, libraries like Pytorch for assisting with deep learning and OpenCV or NumPy. I will also need to download and process the dataset, FaceForensics++, for input into each of the models. I will also need to develop code to make sure the data can be evaluated and tracked and make sure the performance of each model can be visualized.
5. Anticipated Difficulties and Pitfalls: In terms of the experimentation, there might be issues with either of the models in terms of compatibility with the dataset, FaceForensics++. To prevent this from becoming an issue, I will be doing more research and testing small samples of the dataset with the models to ensure proper functionality. I will also need to do some testing to make sure that the performance of the models can be accurately tracked and properly visualized. My main concern will be developing the proper code for this experiment but with a proper schedule and time allocation during the upcoming weeks, I can avoid any significant last minute disruptions.

References

|  |  |
| --- | --- |
| [1] | K. Z. X. R. S. &. S. J. He, "Deep residual learning for image recognition," *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition,* pp. 770-778, 2016. |
| [2] | W. F. X. D. E. D. C. A. S. T.-Y. L. J. S. B. Z. Irwan Bello, "Revisiting ResNets: Improved Training and Scaling Strategies," *Advances in Neural Information Processing Systems,* 2021. |
| [3] | M. Tan, "Efficientnet: Rethinking model scaling for convolutional neural networks," *eprint arXiv:1905.11946,* 2019. |
| [4] | M. a. Q. L. Tan, "Efficientnetv2: Smaller models and faster training," *International conference on machine learning,* pp. pp. 10096-10106, 2021. |