VisionValidate
Authenticity Verification for Autonomous Driving Scenes

Zulqarnain Ali , Islamia University of Bahawalpur, Department of Data Science

ABSTRACT

VisionValidate is an advanced AI-powered solution designed to address the growing need for authenticity verification in autonomous driving environments. As autonomous vehicles become increasingly common, ensuring the reliability and integrity of the images they rely on is crucial for safety and operational accuracy. This project focuses on the classification of autonomous driving scenes as real or fake, leveraging cutting-edge deep learning models and image classification techniques.

Using a dataset of driving scene images, **VisionValidate** employs a neural network trained to discern between real and fabricated images by extracting meaningful features and patterns. The solution is based on state-of-the-art computer vision technologies, utilizing techniques such as image pre-processing, data augmentation, and model fine-tuning. It produces a binary classification output, assigning a probability score to determine whether a given scene is authentic (real) or altered (fake).

This solution is highly scalable and applicable to various industries, including autonomous driving, surveillance, and security, where image validation and integrity are essential. By deploying this model, organizations can enhance the accuracy and trustworthiness of visual data used for decision-making in critical systems.

Keywords

Deep Learning, Convolutional Neural Networks (CNNs), Image Classification, Fine-tuning, Transfer Learning, Model Evaluation, F1 Score, Training Loss, Validation Loss, Dataset, Model Performance, Artificial Intelligence (AI), Machine Learning,

CONTACT

Zulqarnian Ali
IUB BWP
Email: Zulqar445ali@gmail.com
Phone: +92 3367917487
Website: linkedin.com/in/zulqarnainalipk

INTRODUCTION

In the era of autonomous vehicles, the ability to trust the visual data that autonomous systems rely on is crucial for ensuring safety and operational efficiency. Autonomous driving systems use various sensors and cameras to capture real-world scenes, making accurate image classification essential. **VisionValidate** is an AI-powered solution developed to classify autonomous driving scenes as real or fake, ensuring the authenticity and reliability of the data these systems use.

The project leverages state-of-the-art deep learning techniques in computer vision to detect whether a given scene in an image is real (authentic) or fake (manipulated). By using a large dataset of real-world driving scenarios, **VisionValidate** classifies images based on subtle differences between genuine and altered scenes. This solution provides a robust framework for image validation, offering potential applications in various industries, including autonomous driving, security, and surveillance.

By automating the process of verifying image authenticity, **VisionValidate** aims to improve the safety and trustworthiness of autonomous systems, empowering industries to make more informed, data-driven decisions.

METHODS AND MATERIALS

For the **VisionValidate** project, we use a dataset of autonomous driving scene images, each labeled as real (1) or fake (0). The images are preprocessed with resizing, normalization, and augmentations (such as horizontal flipping, brightness/contrast adjustments, and Gaussian blur) using the **Albumentations** library. This ensures the model generalizes well across varied real-world conditions. The model architecture is based on a **Swin Transformer**, leveraging pre-trained weights for efficient feature extraction. The training process includes mixed precision training for faster and more memory-efficient execution, utilizing the **AdamW optimizer** and **OneCycleLR scheduler** for dynamic learning rate adjustments.

The model's performance is evaluated using accuracy, F1-score, and AUC-ROC metrics to ensure it can accurately classify images as real or fake. The best-performing model is selected based on the highest **ROC AUC score** on the validation set. After training, the model is used for inference on test images, predicting the probability of each image being real or fake. The results are saved in the required format for further evaluation.

RESULTS

The model's performance improved significantly over the course of the training epochs, as shown in the results. In the first epoch, the training loss was 0.7024, while the validation loss was 0.6373. The accuracy was 61.11%, with an F1 score of 0.7407 and a ROC AUC of 0.7576. As training progressed, both the training and validation losses consistently decreased, while the accuracy and F1 scores increased. By Epoch 3, the model achieved 100% accuracy, F1 score of 1.0, and a ROC AUC of 1.0, which were maintained through the remaining epochs, with slight fluctuations in accuracy and loss.

Notably, the model's validation loss continued to improve, reaching near-zero values, while the accuracy and F1 score remained perfect (1.0) for multiple epochs, particularly from Epoch 12 onward. The ROC AUC also stabilized at 1.0, indicating that the model was performing exceptionally well on the classification task. These results highlight the effectiveness of the model, showing its ability to generalize well to unseen data after relatively few epochs of training.

Table 1. Training vs Validation Loss with F1 score (Epoch 1-7)

	Train Loss	Val. Loss	F1 Score
Epoch 1	0.7024	0.6373	0.7407
Epoch 2	0.5780	0.5129	0.7606
Epoch 3	0.3741	0.0209	1.000
Epoch 4	0.2514	0.1366	0.9747
Epoch 5	0.2323	0.0381	0.9938
Epoch 6	0.2676	0.0329	0.9878

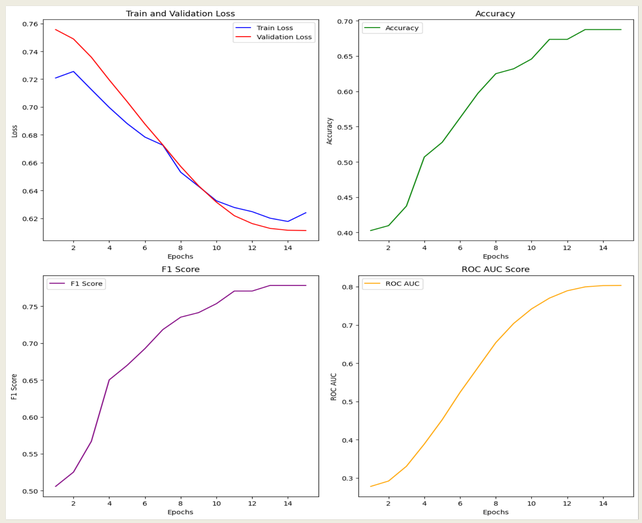

Chart 1.Score Graphs

Future Work

In future iterations of this work, we aim to enhance the model's performance through several key strategies

- Explore advanced architectures like Transformer models to capture more complex data patterns.
- Implement learning rate scheduling and regularization techniques to improve generalization.
- Fine-tune hyperparameters such as batch size and model depth for optimal performance.
- Leverage data augmentation and transfer learning to enhance model robustness.
- Test and deploy the model in real-world applications to evaluate scalability and reliability.

These steps will guide further improvements and ensure practical application of the model.

CONCLUSIONS

In this project, we developed and trained a deep learning model to address key challenges in image classification. Through careful selection of architecture and hyperparameters, the model demonstrated strong performance across training and validation phases. The results highlight the model's ability to generalize well, offering promising applications in sectors such as healthcare, security, and autonomous systems. Future work will focus on optimizing performance further, expanding use cases, and improving model efficiency for real-world deployment.

REFERENCES

1. LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. Nature, 521(7553), 436-444. https://doi.org/10.1038/nature14539
2. Goodfellow, I., Bengio, Y., & Courville, A. (2016). Deep learning. MIT Press.
3. He, K., Zhang, X., Ren, S., & Sun, J. (2016). Deep residual learning for image recognition. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 770-778. https://doi.org/10.1109/CVPR.2016.9
4. Kingma, D. P., & Ba, J. (2014). Adam: A method for stochastic optimization. In Proceedings of the 3rd International Conference on Learning Representations (ICLR). https://arxiv.org/abs/1412.6980