Spoofing AI Image Processing Techniques for Lane Detection

Shelaniece Clash-Morgan State University
shcla13@morgan.edu
Advisor Dr. Kevin Kornegay
Department of Electrical and Computer Engineering (ECE)

Abstract

Autonomous vehicles have been regarded as the ultimate solution to future automotive engineering. Lane detection is a required task for vehicles to navigate autonomously, since the results directly affect steering decisions. Lane detection methods based on computer vision and image processing can be divided into two categories: the traditional image processing and semantic segmentation methods.

Traditional machine learning methods and deep learning Convolutional Neural Network (CNN) models are the basis of this research. Traditional machine learning algorithms for lane detection are manually tuned parameters for feature extraction. The image was pre-processed using grayscale, noise filtering, and edge detection to obtain the edge points of the lane lines.

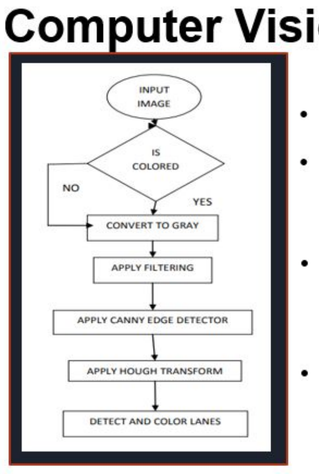
A Convolutional Neural Network eliminates the need for manual feature extractions. This deep learning architecture for lane detection is a predictive model that is consistently fed data to improve the car's predictive abilities. This deep learning approach uses segmentation techniques for lane detection. The Convolutional Neural Network model was investigated, visualizing the weaknesses of lane detection patterns when camera filters alter images after training the neural network.

In this work, conventional lane detection and deep learning models process the image-based dataset. These models present vulnerabilities in popular lane detection algorithms. The vulnerabilities arise from the variability of the road condition in traditional lane detection. Adding camera filters to images after the neural network has been trained caused uncertainty when visualizing weaknesses in pattern data. An investigation to determine the security of computer vision image processing for lane detection aims to promote public trust in automated driving and improve the accuracy of lane detection algorithms. Finally, we present work in progress, survival techniques to advance the security issues of spoofed image processing techniques for lane detection.

Index Terms—Lane Detection, Adversarial Attack, Machine Learning, Neural Network

Conventional Lane Detection (Results)

Computer Vision: Lane Detection



- Image
- Canny Edge Detection
- Region of interest
- Lane Detection

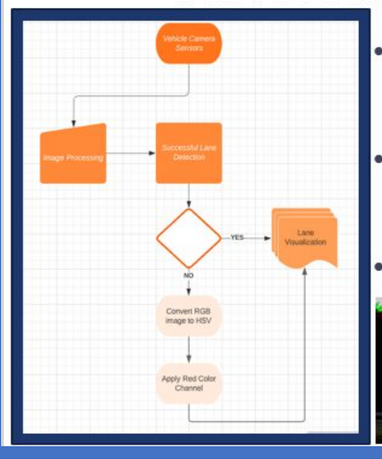
Adversarial Attack Example

- Lane Detection adding a reflective natural surface

- Lane line algorithm disruption after reflective natural surface

To defend against this attack, the vision algorithm must know what this vulnerability is and what the outcome will be if the attack is not corrected. The autonomous vehicle must terminate the program and pass the driving to the occupant or must implement a secondary solution. The complexity of water makes it hard for the algorithm to differentiate the painted lane lines as water is reflective and refractive. A technique to remove glare from an image was used to solve the problem.

Adversarial Attack Defense

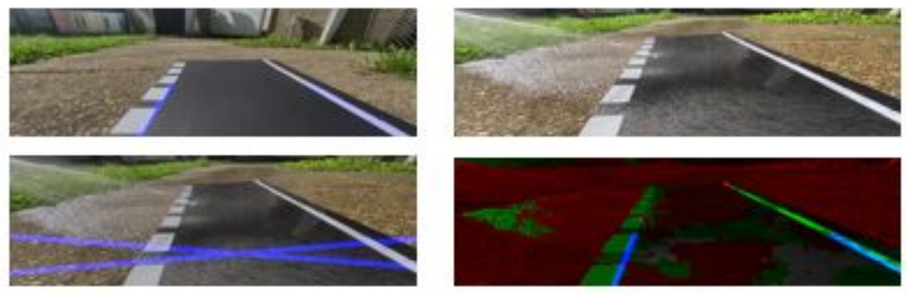


- **Convert image from RGB color space to Hue Saturation Value (HSV) color space**
  - Filter pixels
- **Apply red color filter**
  - The longest wavelength of visible light in the color spectrum.
- **Corrected lane lines visualization**

Images:	Left Lane Line	Right Lane Line	Results
Lane Lines detected	-1.10, 845.95	0.99, -426.34	Original Image
Water, lane lines not properly detected	-0.78, 681.91	0.17, 154.78	The lane lines deviated from the the original image
Water, color channel, lane lines visualized	-1.07, 830.96	1.17, -540.71	The lane line detected in the red channel image. Very slight deviation from lane fit line of original image not visualized in the image.

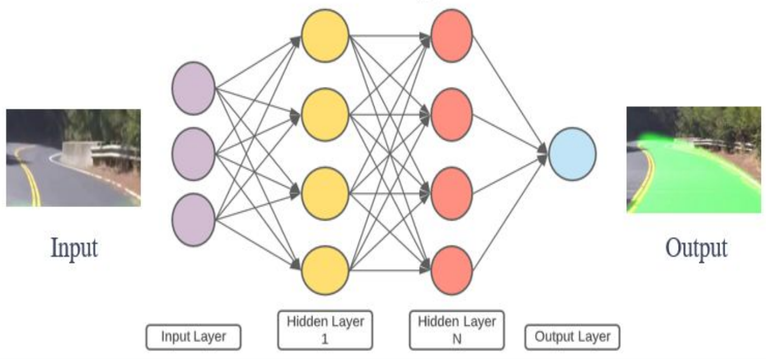
Table 1: Left and Right Fit Lane Lines

Will the provided solution improve the detection capabilities when the surface is wet?



Convolutional Neural Network Lane Segmentation (Results)

Convolutional Neural Network Lane Detection Algorithms

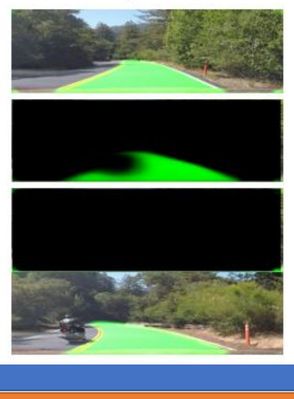


Adversarial Attack Example (CNN Method)

Lane Detection

Added Fisheye filter after CNN training

Adversarial Attack Example (CNN Method blackout filter)



- Lane Segmentation
- Images 0-2, as the neural network tries to detect the lane.
- Images 3-9 (no detection)
- Detection after 10th blacked out image

Conclusion

The experimental results in the CNN model show that the lane detection module can be deceived. When the conventional method encountered the water or hyper-reflective surface in the roadway, the lane lines are incorrectly visualized and placed sporadically on the image. The proposed defense of changing the image filter to a red color channel, removing noise from the image, and reducing the reflection within the image can defend against this type of adversarial attack with minimal impact to lane detection capabilities.

References

[1] A. Geiger, P. Lenz, and R. Urtasun, "Are we ready for autonomous driving? the kitti vision benchmark suite," in 2012 IEEE conference on computer vision and pattern recognition. IEEE, 2012, pp. 3354–3361.
[2] A. S. Rathore, "Lane detection for autonomous vehicles using opencv library," International Research Journal of Engineering and Technolog, vol. 6, no. 1, pp. 1326–1332, 2019.
[3] Y. Ko, Y. Lee, S. Azam, F. Munir, M. Jeon, and W. Pedrycz, "Key points estimation and point instance segmentation approach for lane detection," IEEE Transactions on Intelligent Transportation Systems, 2021.