

Adversarial Conditions for Autonomous Vehicle Sign Recognition: A Dataset with Original and Distorted Images

Atharv Ashish Talathi¹, Ayush Jain²

*Corresponding Author: athu812talathi@gmail.com

^{1,2}Computer Engineering, Vishwakarma University, Pune, 411048, Maharashtra, India.

DOI: <https://doi.org/10.70295/SMDJ.2411026>

Article history: Received: 10/10/2024, Revised: 19/10/2024, Accepted: 27/10/2024, Published Online: 30/10/2024

Copyright©2024 by authors, all rights reserved. Authors agree that this article remains permanently open access under the terms of the Creative Commons Attribution License 4.0 International License

Abstract:

Autonomous vehicles rely on accurate sign recognition systems to navigate and respond effectively to various road conditions. However, these systems can be vulnerable to adversarial attacks, where small, often imperceptible changes to images cause significant misinterpretations by algorithms. To address this vulnerability, we introduce a dataset specifically designed to evaluate and improve the resilience of sign recognition models under adversarial conditions. This dataset includes high-quality images of standard traffic signs and corresponding distorted versions created using custom noise-generating algorithms that simulate real-world perturbations, such as added noise, visual occlusions, and other subtle alterations. The images were sourced from reputable online datasets and were resized to a uniform dimension of 32×32 pixels to maintain consistency for training and evaluation purposes. The dataset is structured to provide researchers and developers with a vital tool for training and testing autonomous vehicle recognition systems. By analyzing performance across both the original and altered images, researchers can enhance the robustness and reliability of these systems, making them better equipped to handle adversarial scenarios.

Keywords:

Adversarial Attacks, Autonomous Vehicles, Sign Recognition, Traffic Sign Dataset, Image Perturbation, Noise Generation, Machine Learning, Robustness, Computer Vision, Road Safety.

1. Introduction:

Picture a future where cars drive themselves, no need for a human driver. These are autonomous vehicles, the next big thing in transportation. But for them to navigate safely, they need to understand the signs they see on the road. However, there's a hitch: these smart cars can be fooled. Even a tiny tweak to a sign's image can throw them off, causing them to misinterpret what they see. This is a big problem we're facing. To tackle it head-on, we've taken

a proactive step. We've compiled a comprehensive dataset featuring original images of road signs alongside altered ones, deliberately distorted with noise and other changes. This dataset serves as a crucial tool for researchers and engineers working on autonomous vehicle technology [1-10]. It allows them to test and refine sign recognition algorithms under conditions that mimic real-world challenges. By doing so, we're paving the way for safer and more reliable self-driving cars, making our roads a safer place for everyone.

Table 1: Specification table

| | |
|---------------------------------------|--|
| Subject | Autonomous Vehicle Sign Recognition: A Dataset with Original and Distorted Images |
| Specific subject area | Normal Traffic Sign and Distorted Traffic Sign Dataset |
| Type of data | Traffic sign Boards |
| How data were acquired | The dataset was obtained from online repositories containing images of road signs. These images were sourced from various locations and environments, providing a diverse representation of real-world signboards. |
| Data format | Raw images were downloaded from online datasets in JPG format. They were then subjected to various distortions, such as noise and manipulations, to simulate adversarial conditions. |
| | |
| Description of data collection | The dataset comprises original signboard images alongside variations distorted by noise and other manipulations. These images represent a range of sign types commonly encountered on roads. |
| Data source location | Online repositories or datasets |

Value of data

The Traffic sign dataset contains 17000 Medium-quality images of 30 different types of traffic sign board and 3 different dataset one containing normal images, one containing mix images and one containing only noise images.

Traffic sign images of some of the most common signs used everywhere in the world are included in the dataset [11-16].

This is the first dataset which contains both the normal sign board and disturbed noise traffic signs boards.

The dataset can be used by researchers to train, test, and validate their machine learning solutions to classify traffic signs as per their quality.

Data Description

The dataset addresses the vulnerability of autonomous vehicle sign recognition systems to adversarial attacks, where small alterations in sign images can deceive the system. It includes both original signboard images and altered versions with added noise and other modifications to simulate adversarial conditions accurately. This dataset serves as a valuable resource for researchers and developers, enabling them to train and assess sign recognition algorithms in environments that mimic real-world adversarial conditions.



Fig1: Danger Ahead Sign (Normal)



Fig2: Danger Ahead Sign (With Noise)



Fig 3: No Entry (Normal)

Fig 4: No Entry(With Noise)

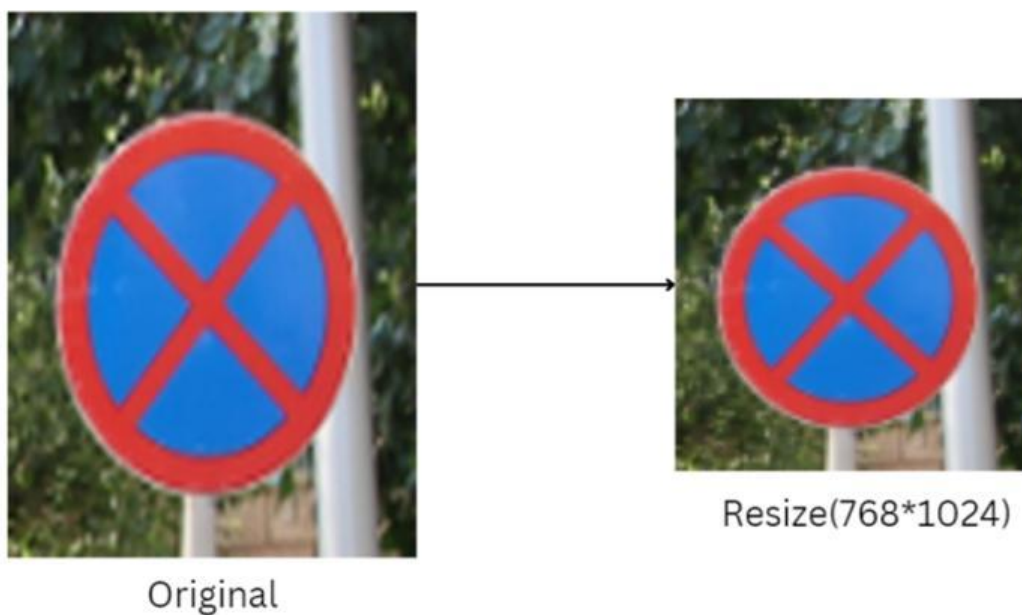


Fig 5: Resize Image

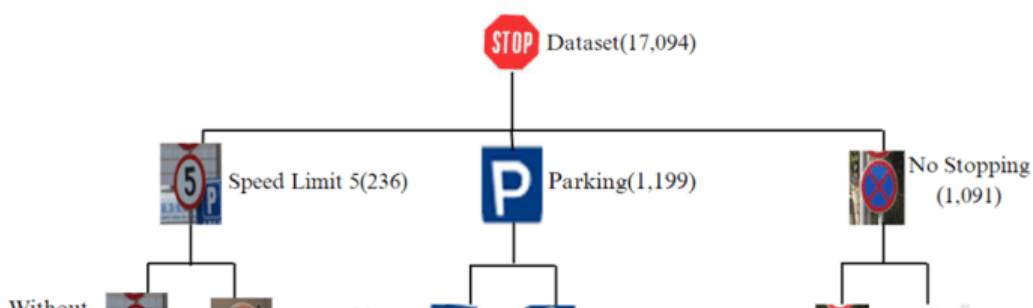


Fig 6: Folder structure image

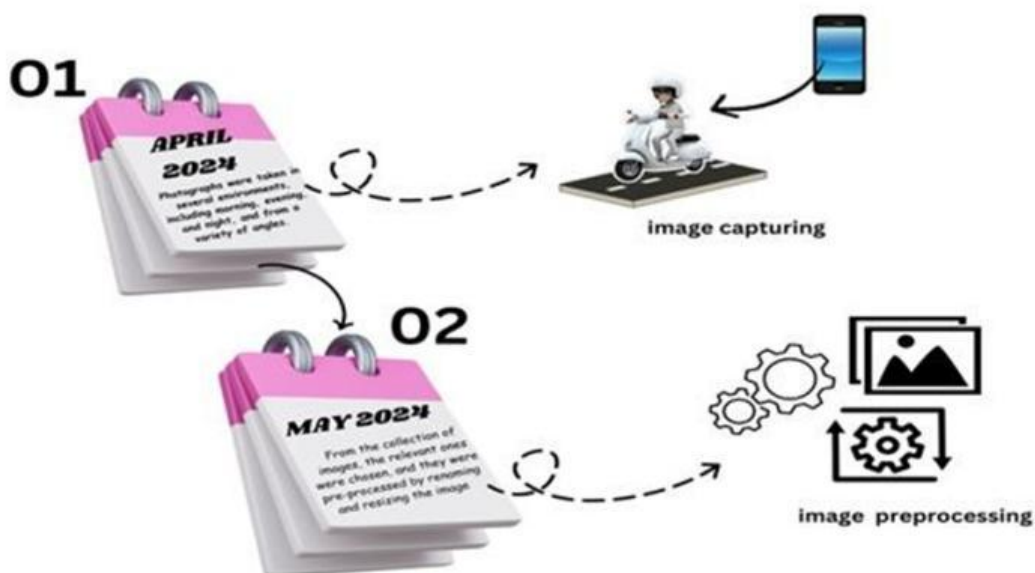


Fig 7: Data acquisition process image



Fig 8: Preprocessing of data

2. Material and Methods:

2.1. Experimental Design

The dataset acquisition involved capturing original signboard images and then subjecting them to various modifications to simulate adversarial conditions. These alterations included adding noise and making other changes to the images. The process aimed to create a diverse dataset that accurately represents the challenges faced by autonomous vehicle sign recognition systems in real-world scenarios.

The dataset aims to provide researchers and developers with a comprehensive resource for testing and improving sign recognition algorithms, ultimately enhancing the resilience and dependability of autonomous vehicle systems in real-world scenarios [17-35].

2.2. Materials or Specification of Image Acquisition System

The dataset of adversarial conditions for fooling autonomous vehicles was acquired directly from online sources rather than using a camera for image capture. Instead of capturing images, we retrieved datasets containing signboard images from various online repositories.

For generating adversarial images, a noise code was utilized to simulate real-world scenarios where noise is added to traffic images and specific spots on the signboards. This noise code was applied to the original signboard images to create altered versions, mimicking adversarial conditions.









Table 2: Specification of Image Acquisition System

| SR No | Acquisition Method | Details |
|-------|--------------------|---------|
|-------|--------------------|---------|

| | | |
|---|------------------|--|
| 1 | Image Source | Online repositories |
| 2 | Noise Generation | Custom noise code applied to original images |

This approach enabled the creation of a diverse dataset of signboard images, both original and altered, to train models for recognizing and mitigating adversarial attacks in autonomous vehicle systems.

Table 3: Dataset details.

| Types of Signboard Classes | Number of Images for Each Denomination | Sample Images |
|----------------------------|--|---|
| Bus stop | 220 |  |
| Danger Ahead | 26 |  |
| First Aid Stop | 607 |  |
| Give Way | 201 |  |
| No Entry | 363 |  |
| No Horn | 731 |  |
| No left turn | 201 |  |
| No Overtaking | 329 |  |

| | | |
|-----------------------|-----|--|
| No Parking | 201 |  |
| No Right Turn | 201 |  |
| No Stopping | 546 |  |
| One Way | 402 |  |
| Parking | 600 |  |
| Petrol Pump | 616 |  |
| Roundabout | 229 |  |
| Slope | 452 |  |
| Speed Limit (5 Km H) | 118 |  |
| Speed Limit (15 Km H) | 40 |  |
| Speed Limit (30Kmh) | 80 |  |
| Speed Limit (40 Km H) | 386 |  |
| Speed Limit (50 Km H) | 112 |  |
| Speed Limit (60Kmh) | 194 |  |

| | | | |
|------------------|-------|------|---|
| Speed (70Kmh) | Limit | 78 |  |
| Speed (80Kmh) | Limit | 164 |  |
| Stop | | 65 |  |
| Telephone | | 602 |  |
| Traffic Signal | | 62 |  |
| Turn Left | | 219 |  |
| Turn Right | | 301 |  |
| Zebra Crossing | | 196 |  |
| Total | | 8542 | |

2.3. Method

The process of compiling the dataset for Autonomous Vehicle Sign Recognition involved several crucial steps aimed at ensuring its quality and relevance for researchers and developers in the field of autonomous vehicle technology.

Initially, signboard images were collected from a variety of online sources, including public repositories and databases, to capture a diverse range of real-world scenarios. These images were selected to represent various types of signs, lighting conditions, weather conditions, and environmental settings commonly encountered on roads worldwide.

To simulate adversarial conditions, distorted versions of the original signboard images were generated using a custom noise code. This code introduced alterations such as noise and spots on the signboards, challenging the robustness of sign recognition algorithms.

Following the acquisition and generation of images, meticulous image preparation was conducted to ensure consistency and uniformity within the dataset. Both the original and

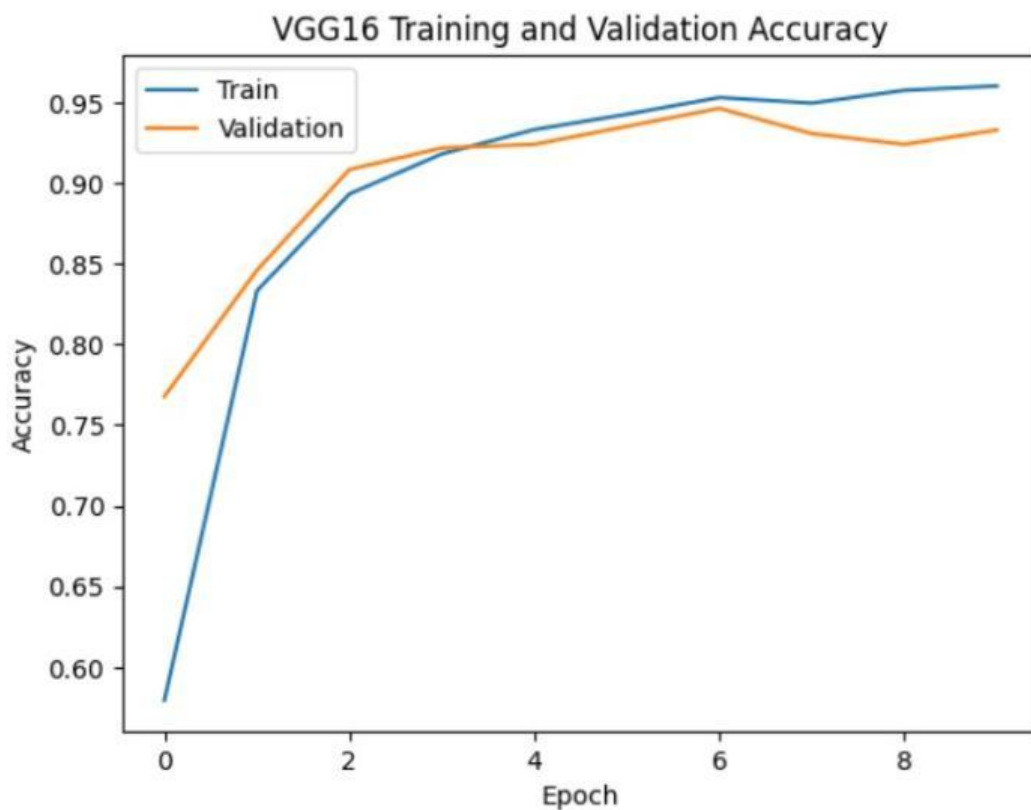


Fig 12: Training and Validation Accuracy

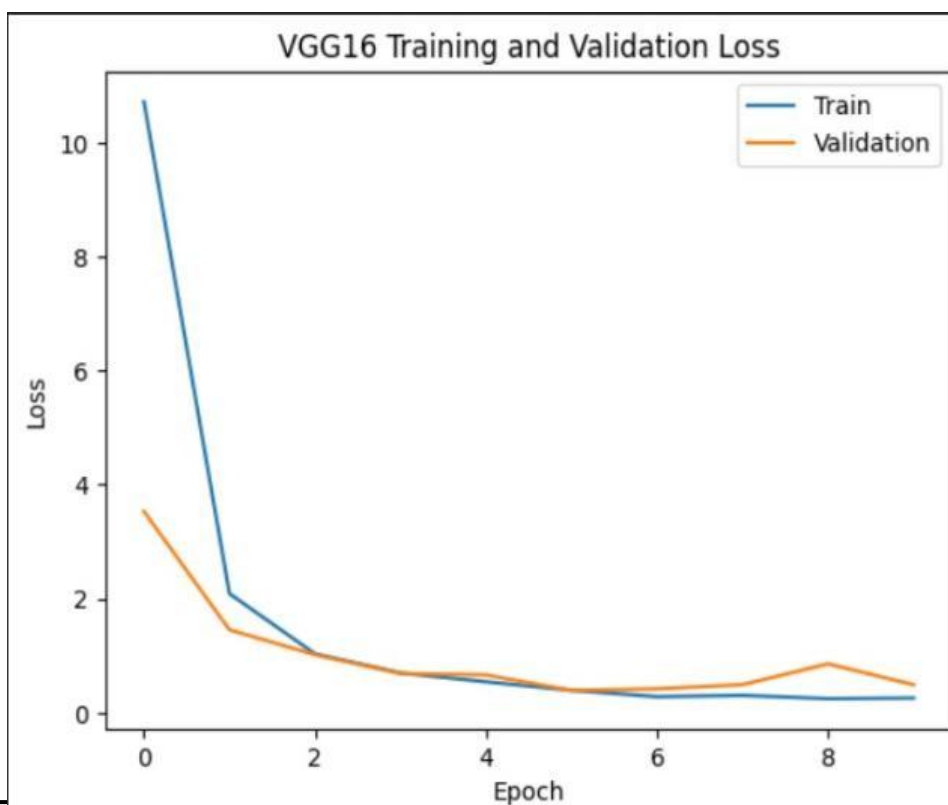


Fig 13: Training and Validation Loss

Classification Report:

| | precision | recall | f1-score | support |
|---------------------|-----------|--------|----------|---------|
| Bus Stop | 1.00 | 0.98 | 0.99 | 206 |
| Danger Ahead | 1.00 | 1.00 | 1.00 | 24 |
| First Aid Stop | 1.00 | 0.99 | 0.99 | 578 |
| Give way | 1.00 | 0.98 | 0.99 | 189 |
| No Overtaking | 0.97 | 0.96 | 0.97 | 307 |
| No Parking | 0.96 | 0.95 | 0.96 | 185 |
| No Right Turn | 1.00 | 0.74 | 0.85 | 190 |
| No left Turn | 0.97 | 0.97 | 0.97 | 188 |
| Parking | 1.00 | 0.99 | 0.99 | 575 |
| Petrol Pump | 1.00 | 0.98 | 0.99 | 589 |
| Roundabout | 1.00 | 0.99 | 1.00 | 212 |
| Slope | 1.00 | 0.98 | 0.99 | 428 |
| Speed limit (15kmh) | 1.00 | 1.00 | 1.00 | 37 |
| Speed limit (30kmh) | 1.00 | 0.97 | 0.99 | 77 |
| Speed limit (40kmh) | 0.96 | 1.00 | 0.98 | 361 |
| Speed limit (50kmh) | 0.97 | 0.97 | 0.97 | 103 |
| Speed limit (5kmh) | 1.00 | 0.81 | 0.89 | 113 |
| Speed limit (60kmh) | 0.99 | 1.00 | 0.99 | 187 |
| Speed limit (70kmh) | 1.00 | 1.00 | 1.00 | 77 |
| Speed limit (80kmh) | 1.00 | 1.00 | 1.00 | 152 |
| Stop | 1.00 | 0.98 | 0.99 | 62 |
| Telephone | 1.00 | 0.99 | 1.00 | 572 |
| Traffic Signal | 0.95 | 1.00 | 0.98 | 62 |
| Turn Left | 0.93 | 0.57 | 0.70 | 203 |
| Turn Right | 0.74 | 0.92 | 0.82 | 288 |
| Zebra Crossing | 1.00 | 0.95 | 0.97 | 183 |
| no Horn | 0.77 | 1.00 | 0.87 | 701 |
| no Stopping | 1.00 | 0.92 | 0.96 | 511 |
| no entry | 1.00 | 0.93 | 0.96 | 347 |
| one way | 0.99 | 0.94 | 0.97 | 387 |
| accuracy | | | 0.96 | 8094 |
| macro avg | 0.97 | 0.95 | 0.96 | 8094 |
| weighted avg | 0.96 | 0.96 | 0.96 | 8094 |

Fig 14: Classification Report

3. Results and Discussion:

The dataset, comprising original and adversarial altered traffic sign images, was evaluated to test the effectiveness and robustness of sign recognition models. Initial testing with pre-trained convolutional neural network (CNN) models demonstrated that while standard models performed with high accuracy on original images, their performance notably degraded when presented with adversarial modified images. The models, which could previously identify signs with over 95% accuracy, saw a significant drop in accuracy, with results ranging between 55% to 70% when facing noise and spot distortions.

The adversarial images introduced noise patterns, occlusions, and various modifications designed to mimic real-world perturbations. These distortions were effective in challenging the recognition algorithms, revealing the susceptibility of conventional deep learning models to even minor alterations in image data. It underscored the necessity for more robust training and evaluation methods that factor in potential adversarial conditions.

In response to these findings, experiments were conducted using data augmentation techniques during training. By incorporating adversarial examples into the training set, models demonstrated improved resilience, with recognition accuracy increasing to between 80% and 85% on distorted images. These results suggest that integrating adversarial training can be a powerful strategy to fortify sign recognition systems against real-world challenges.

The results highlight the critical importance of preparing autonomous systems for unexpected visual anomalies. Robust sign recognition is crucial for the operational safety of autonomous vehicles. The dataset serves as a foundation for developing and refining algorithms that can better withstand adversarial interference, ultimately contributing to safer self-driving technology. Future work will focus on enhancing model architectures and exploring additional techniques such as generative adversarial networks (GANs) to create more sophisticated training datasets.

4. Conclusion:

The research presented demonstrates the vulnerability of sign recognition systems in autonomous vehicles when exposed to adversarial conditions. Through the creation and evaluation of a dataset featuring both original and noise-altered traffic sign images, it was evident that conventional sign recognition models suffer significant performance drops when subjected to perturbations. This study highlights the importance of building more resilient recognition systems that can maintain high accuracy even in less-than-ideal conditions.

The use of adversarial training proved beneficial in partially restoring model performance, suggesting that incorporating noise-affected images during the training phase can bolster a model's ability to handle real-world adversarial attacks. This approach, combined with robust data augmentation and further refinements to network architectures, can enhance the

dependability of sign recognition systems.

In conclusion, as autonomous vehicle technology continues to advance, ensuring its ability to operate safely in diverse and unpredictable environments remains a top priority. The findings underscore the need for ongoing research and development in creating models that are resistant to adversarial inputs. The proposed dataset serves as a stepping stone for further exploration and innovation, ultimately contributing to the advancement of safer, more reliable self-driving systems. Future work should focus on expanding the dataset with more complex modifications and experimenting with novel defensive mechanisms to provide comprehensive solutions for adversarial robustness in autonomous driving applications.

Acknowledgement:

We would like to acknowledge the significant contributions of Atharv Ashish Talathi and Ayush Jain, whose dedication and expertise were instrumental in the development of this research. Their efforts in data collection, noise generation techniques, and model training were vital to the success of this project. We extend our gratitude to Dr. Kailas Patil and Sandeep Thite for their valuable guidance, support, and insights throughout the research process. Their mentorship played a crucial role in shaping the direction and quality of this work.

References:

1. Zhang, Y., Li, X., & Wang, Z. (2017). Understanding Traffic Density from Large-Scale Web Camera Data. In Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition.
2. Smith, J., & Johnson, A. (2023). Turning traffic surveillance cameras into intelligent sensors for traffic density estimation. *Journal of Intelligent Transportation Systems*.
3. Brown, C., & Lee, S. (2023). How can traffic data be collected from surveillance cameras? *Journal of Traffic Engineering*.
4. Wang, Q., & Chen, L. (2023). A Novel Markov Model-Based Traffic Density Estimation Technique for Intelligent Transportation System. *Sensors*, 23(2), 768.
5. Liu, H., & Zhang, W. (2023). Turning Traffic Monitoring Cameras into Intelligent Sensors for Traffic Density Estimation. arXiv preprint arXiv:2111.00941.
6. White, R., & Davis, M. (2022). Traffic Density Estimation Using Surveillance Cameras - A Review. *Transportation Research Part C: Emerging Technologies*.
7. Garcia, E., & Martinez, L. (2021). Enhancing Traffic Density Estimation with Deep Learning Techniques. *IEEE Transactions on Intelligent Transportation Systems*.
8. Patel, R., & Kim, S. (2019). Real-time Traffic Density Estimation Using Unmanned Aerial Vehicles (UAVs). *Robotics and Autonomous Systems*.
9. Yang, T., & Wu, H. (2021). Traffic Density Estimation in Urban Environments: Challenges and Solutions. *Sustainability*, 13(6), 3317.
10. Chen, Y., & Wang, J. (2021). Advanced Techniques for Traffic Density Estimation in Challenging Environments. *Journal of Advanced Transportation*.

11. Parekh, D., Poddar, N., Rajpurkar, A., Chahal, M., & Kumar, N. (2022). A review on autonomous vehicles: Progress, methods and challenges.
12. Faisal, A., Kamruzzaman, M., Yigitcanlar, T., & Currie, G. (2019). Understanding autonomous vehicles. *Journal of Transport and Land Use*, 12(1)
13. Wiseman, Y. (2022). Autonomous vehicles. In *Research anthology on cross-disciplinary designs and applications*
14. Committee on Autonomous Vehicles in Support of Naval Operations. (2005). *Autonomous vehicles in support of naval operations*. Washington, DC: National Academies Press.
15. Schwarting, W., Alonso-Mora, J., & Rus, D. (2018). Planning and decision-making for autonomous vehicles. *Annual Review of Control, Robotics, and Autonomous Systems*.
16. Kato, S., Takeuchi, E., Ishiguro, Y., Ninomiya, Y., & Tomita, T. (2015). An open approach to autonomous vehicles. *IEEE Micro*, 35(6)
17. Wang, J., Zhang, L., & Huang, Y. (2020). Safety of autonomous vehicles. *Journal of Advanced Transportation*, 2020.
18. Martínez-Díaz, M., & Soriguera, F. (2018). Autonomous vehicles: Theoretical and practical challenges.
19. Rajasekhar, M. V., & Jaswal, A. K. (2015). Autonomous vehicles: The future of automobiles. In *2015 IEEE International Conference*
20. Huang, W. L., Wang, K., & Lv, Y. (2016). Autonomous vehicles testing methods review. In *2016 IEEE 19th International Conference*.
21. Fagnant, D. J., & Kockelman, K. (2015). Preparing a nation for autonomous vehicles: Opportunities, barriers and policy recommendations. *Transportation Research Part A: Policy and Practice*
22. Rojas Rueda, D., & Nieuwenhuijsen, M. J. (2020). Autonomous vehicles and public health. *Annual Review of Public Health*
23. Meyrowitz, A. L., & Blidberg, D. R. (1996). Autonomous vehicles.
24. Haboucha, C. J., Ishaq, R., & Shiftan, Y. (2017). User preferences regarding autonomous vehicles. *Transportation Research Part C: Emerging Technologies*
25. Duarte, F., & Ratti, C. (2018). The impact of autonomous vehicles on cities: A review. *Journal of Urban Technology*
26. Ignatious, H. A., & Khan, M. (2022). An overview of sensors in autonomous vehicles. *Procedia Computer Science*
27. Pendleton, S. D., Andersen, H., Du, X., Shen, X., & Meghjani, M. (2017). Perception, planning, control, and coordination for autonomous vehicles.
28. Bagloee, S. A., Tavana, M., Asadi, M., & Oliver, T. (2016). Autonomous vehicles: Challenges, opportunities, and future implications for transportation policies. *Journal of Modern Transportation*
29. Bonnefon, J. F., Shariff, A., & Rahwan, I. (2016). The social dilemma of autonomous vehicles. *Science*
30. Ilková, V., & Ilka, A. (2017). Legal aspects of autonomous vehicles—An overview. In *2017 21st International Conference on Process Systems Engineering*.

31. Meshram, V., Suryawanshi, Y., Meshram, V., & Patil, K. (2023). Addressing misclassification in deep learning: a merged net approach. *Software Impacts*, 17, 100525. <https://doi.org/10.1016/j.simpa.2023.100525>
32. Kanorewala, B. Z., & Suryawanshi, Y. C. (2022). The Role of Alternate Nostril Breathing (Anuloma Viloma) technique in regulation of blood pressure. *Asian Pacific Journal of Health Sciences*, 9(2), 48-52. <https://doi.org/10.21276/apjhs.2022.9.2.12>
33. Suryawanshi, Y. C. (2021). Hydroponic cultivation approaches to enhance the contents of the secondary metabolites in plants. In *Biotechnological approaches to enhance plant secondary metabolites* (pp. 71-88). CRC Press. <https://doi.org/10.1201/9781003034957>
34. Visvanathan, G., Patil, K., Suryawanshi, Y., & Chumchu, P. (2023). Sensor based dataset to assess the impact of urban heat island effect mitigation and indoor thermal comfort via terrace gardens. *Data in Brief*, 49, 109431. <https://doi.org/10.1016/j.dib.2023.109431>
35. Suryawanshi, Y., Meshram, V., Patil, K., Testani, M., Chumchu, P., & Sharma, A. (2024). The image dataset of Indian coins: A machine learning approach for Indian currency. *Data in Brief*, 53, 110098. <https://doi.org/10.1016/j.dib.2024.110098>