2022-01-0115 Published 29 Mar 2022

Securing Camera Based Active Driver Monitoring System from Video Forgery Attacks Using Deep Learning

Prashanth K. Y. Rao Bahadur Y Mahabaleswarappa Engineering College

Rohitha Ujjini Matad Proudadevaraya Institute Of Technology

Sarala S M Ramaiah Institute Of Technology

Citation: Prashanth, K.Y., Ujjini Matad, R., and Sarala, S.M., "Securing Camera Based Active Driver Monitoring System from Video Forgery Attacks Using Deep Learning," SAE Technical Paper 2022-01-0115, 2022, doi:10.4271/2022-01-0115.

Received: 20 Jan 2022 Revised: 20 Jan 2022 Accepted: 17 Jan 2022

Abstract

The numerous superiorities of autonomous vehicles in terms of safety, driving experience, and comfort against the traditional driving favor them in the wide adoption across the modern automotive sector. Driver Monitoring System (DMS) is one of the high Automotive Safety Integrity Level (ASIL) specified driver assistance functionalities, which assists the driver continuously as a part of Active Safety system. The fused vision-related functionalities of the camera based active DMS such as Distraction, Drowsiness, and Emotion detection systems monitors the driver's In-vehicle Activities, Eye movements, and Facial expressions respectively to awake the driver with constant alerts under undesired conditions to achieve a right driving attention. The presence of the modern day DMS in the In-Vehicle-Infotainment Digital Cockpits exposes the critical DMS into a wide range of cyber-attacks either locally or remotely, which in turn causes the malfunctioning of the active safety driver assistance system. This malfunctioning is due to integrity compromisations through cyberattacks, where attackers forge the incoming driver video data on the compromised infotainment system, which has external world connectivity. The tampering of incoming video content which contains driver activities, eye movements, and facial expressions at pixel level, block level or scene results in false interpretation by the distraction, drowsiness, and emotion detection modules of DMS respectively. The false interpretation of the driver states by camera based behavioral active DMS causes numerous false positive and false negative driver alerts due to cyber-attacks, which are undesired. Hence, here a deep learning based digital forensic approach is proposed to detect the forgery attacks on the DMS. The attacker's successful launch of forgery attacks on the driver monitoring video information is detected intelligently using deep learning techniques before passing the video input for DMS modules such as Distraction, Drowsiness, and Emotion detection. The proposed approach involves the detection of splicing and copy-move object forgery attacks on the front camera feeds of the DMS in real-time using convolutional neural networks. The proposed system is responsible for validating the authenticity of the incoming real-time camera video frames prior to Distraction, Drowsiness, and Emotion detections and generating alerts. Hence, the proposed system successfully detects the video forgery attacks, and provides only the authentic driver monitoring alerts by enhancing the trust on driver monitoring systems from cyber-attacks by ensuring the safety and system integrity.

Introduction

The technological crossover of the current trending technologies such as artificial intelligence, internet of things and so on reflects in the evolution of near-human perfectionist autonomous systems across the industries. The automotive industry is moving at a fast pace in achieving the autonomous vehicles by utilizing these powerful technologies. The autonomous vehicles, which are intended to improve the safety, traffic management, and user experience uses multiple sensor-actuator arrangements in emulating the human driving with some additional superiorities. Along with driver safety, an upcoming critical aspect in the vehicular system is the driving comfort. The cognitive study of the driver along with the physical health are drawing research interest for providing the enhanced and safe driving experience for the driver. One of the major human cognitive behaviors, which is critical for driving is the attention, which gets faded as a function of sleep, fatigue, and other medical conditions. In order to meet the level of driving experience along with safety, numerous understanding and modelling of the vehicular environment, which is a combination of driver, vehicle, and dynamic environment is required. This research topic is a

References

1. Euro NCAP. "Technical Papers—Euro NCAP 2025 Roadmap (2017, 09)," Available online: https://cdn.euroncap.com/media/30700/euroncap-roadmap-2025-v4.pdf.
2. Sikander G. and Anwar S., "Driver Fatigue Detection Systems: A Review," in *IEEE Transactions on Intelligent Transportation Systems*, vol. 20, no. 6, pp. 2339-2352, June 2019, doi: 10.1109/TITS.2018.2868499.
3. Ngxande M., Tapamo J. and Burke M., "Driver Drowsiness Detection Using Behavioral Measures and Machine Learning Techniques: A Review of State-Of-Art Techniques," in *2017 Pattern Recognition Association of South Africa and Robotics and Mechatronics (PRASA-RobMech)*, 2017, pp. 156-161, doi: 10.1109/RoboMech.2017.8261140.
4. Kashevnik, A., Shchedrin, R., Kaiser, C., and Stocker, A., "Driver Distraction Detection Methods: A Literature Review and Framework," *IEEE Access* 9 (2021): 60063-60076, doi:10.1109/ACCESS.2021.3073599.
5. Dibaei, Mahdi, Zheng, Xi, Jiang, Kun, Maric, Sasa, et al. "An Overview of Attacks and Defences on Intelligent Connected Vehicles," 2019.
6. Mazloom, S. et al., "A Security Analysis of an In-Vehicle Infotainment and App Platform," *WOOT* (2016).
7. Dadam, S.R., Zhu, D., Kumar, V., Ravi, V. and, Palukuru V.S.S., "Onboard Cybersecurity Diagnostic System for Connected Vehicles," SAE Technical Paper 2021-01-1249, 2021, https://doi.org/10.4271/2021-01-1249.
8. Johnston, P. and Elyan, E., "A Review of Digital Video Tampering: from Simple Editing to Full Synthesis," *Digital Investigation [online]* 29 (2019): 67-81. https://doi.org/10.1016/j.diin.2019.03.006.
9. Singh, R.D. and Aggarwal, N., "Video Content Authentication Techniques: A Comprehensive Survey," *Multimedia Systems* 24 (2018): 211-240. https://doi.org/10.1007/s00530-017-0538-9.
10. Simonyan, K., and Zisserman, A. "Very Deep Convolutional Networks for Large-Scale Image Recognition," arXiv preprint arXiv:1409.1556, 2014.
11. Dong, J., Wang, W., and Tan, T. (2013). "CASIA Image Tampering Detection Evaluation Database," 422-426. 10.1109/ChinaSIP.2013.6625374.
12. Silva, E., Carvalho, T., Ferreira, A., and Rocha, A., "Going Deeper into Copy-Move Forgery Detection: 27 Exploring Image Telltales Via Multi-Scale Analysis and Voting Processes," *J. Vis. Commun. Image Represent.* 29 (2015): 16-32.
13. Ortega, J., Kose, N., Cañas, P., Chao, M.A. et al. (2020). "DMD: A Large-Scale Multi-Modal Driver Monitoring Dataset for Attention and Alertness Analysis," in *Proceedings of the European Conference on Computer Vision (ECCV) Workshops*.
14. Lopes A.T., de Aguiar E., De Souza A.F. et Oliveira-Santos T., "Facial Expression Recognition with Convolutional Neural Networks: Coping with Few Data and the Training Sample Order," *Pattern Recognit.*, vol. 61, pp. 610-628, 2017, doi: 10.1016/j.patcog.2016.07.026.
15. Xing Y., Lv C., Wang H., Cao D., Velenis E. and Wang F., "Driver Activity Recognition for Intelligent Vehicles: A Deep Learning Approach," in *IEEE Transactions on Vehicular Technology*, vol. 68, no. 6, pp. 5379-5390, June 2019, doi: 10.1109/TVT.2019.2908425.
16. Bergasa, L.M., Nuevo, J., Sotelo, M.A., Barea, R. et al., "Real-Time System for Monitoring Driver Vigilance," *IEEE Trans. Intell. Transport. Syst* 7 (2006): 63-77.

Contact Information

Prashanth K Y
Department of Electronics & Communication Engineering
RYM Engineering College
Bellary, India
+91 9980539035
prashanthky2021@gmail.com

Definitions/Abbreviations

ASIL - Automotive Safety Integrity Level

CNN - Convolutional Neural Network

DMS - Driver Monitoring System

ECU - Engine Control Unit

IVI - In-Vehicle Infotainment

SVM - Support Vector Machines

VGG-16 - Visual Geometry Group 16.

Positions and opinions advanced in this work are those of the author(s) and not necessarily those of SAE International. Responsibility for the content of the work lies solely with the author(s).

ISSN 0148-7191