

## Chapter 8

# Minimizing Data Loss by Encrypting Brake–Light Images and Avoiding Rear–End Collisions Using Artificial Neural Network

**Abirami M. S.**

 <https://orcid.org/0000-0002-7401-454X>

*SRM Institute of Science and Technology, India*

**Manoj Kushwaha**

*SRM Institute of Science and Technology, India*

### **ABSTRACT**

*Rear-end collisions are a threat to road safety, so reliable collision avoidance technologies are essential. Traditional systems present several issues due to data loss and privacy concerns. The authors introduce an encrypted artificial neural network (ANN) method to prevent front-vehicle rear-end collisions. This system uses encryption techniques and ANN algorithm to recognize the front vehicle brake light in real time. Information can't be deciphered without the appropriate key using encryption. Intercepting data during transmission prevents reading. The system works day and night. ANN outperforms LR, SVM, DT, RF, and KNN in accuracy. An encrypted ANN-based ML model distinguishes between brake and normal signals. ANN accuracy was 93.7%. Driver receives further alerts to avoid rear-end collisions. This work proposes a lightweight, secure ANN-based brake light picture encryption method. The proposed approach may be applied to other collision circumstances, including side and frontal strikes. The technique would be more adaptable and applicable to many road safety circumstances.*

DOI: 10.4018/979-8-3693-1642-9.ch008

## 1. INTRODUCTION

Rear-end collisions are common and often fatal in third-world nations. In complex surroundings with many unknowns, it might be challenging for conventional systems to reliably identify and predict the likelihood of a rear-end collision. Accidents come from drivers who do not respond quickly enough to potential threats (Feng et al., 2020). Sixty percent of crashes can be avoided with a half-second notice, and an astounding ninety percent can be avoided with a 1.5-second warning (Karungaru et al., 2021). Existing methods for collision detection tend to depend largely on a single intelligence algorithm, despite the advantages that may be gained from using a hybrid approach. Furthermore, they frequently fail to account for adverse weather that might reduce vision, rendering their detection systems useless.

Our encrypted images analysis with Artificial Neural Network (ANN) is capable of doing in-depth analyses, identifying patterns, and making very accurate predictions (Guo et al., 2022). It's like having a very intelligent passenger who can foresee potential accidents. One of the most common causes of accidents on the road is rear-end collisions. Distracted driving, driver weariness, and following too closely are just a few of the causes of these (Shang et al., 2021). To prevent front-vehicle rear-end crashes, we present an encrypted technique with ANN in this research.

If the ANN determines that the driver will not be able to respond quickly enough to avoid a collision, an alarm will be triggered. The findings demonstrated that the proposed method might minimize rear-end accidents by as much as 50%. Rear-end collisions are a major cause of traffic accidents (Shen et al., 2023). They account for about 25% of all traffic fatalities in the United States (Zhang et al., 2022). There are many different things that can lead to rear-end collisions, including distracted driving, exhaustion, and following too closely (Kushwaha, 2023).

There are a number of techniques that can be used to avoid rear-end collisions. These include: The driver should always maintain a safe following distance from the vehicle in front of them. This will give them enough time to react if the vehicle in front of them stops suddenly. The driver should avoid distractions while driving, such as talking on the phone or texting. These distractions can prevent the driver from paying attention to the road and can lead to a rear-end collision. The driver should be aware of their surroundings and be prepared to stop if necessary. This includes being aware of the speed and distance of the vehicles around them.

The use of Artificial Intelligence (AI) to prevent rear-end crashes has gained popularity in current years (Fu et al., 2021; Pu et al., 2021). With the help of AI, we can create systems that study the driving habits of individual motorists and foresee when they will cause an accident (Kushwaha & Abirami, 2023). The data collected by these systems can then be utilized to issue warnings or conduct other preventative measures.

This system makes an effort to detect the brake light coming from the forward vehicle by making use of an ANN Machine Learning (ML) algorithm in real-time (Hadjidimitriou et al., 2020; Yang et al., 2020). The accuracy of the ANN method is superior to that of other ML classifiers, including Logistic Regression (LR), Support Vector Machine (SVM), Decision Tree (DT), Random Forest (RF), and K-Nearest Neighbor (KNN), Naïve Bayes (NB), Decision Tree (DT), Stochastic gradient Descent (SGD), Gradient Boosting (GB), AdaBoost. In order to distinguish between normal and brake signals, ML model based on ANN is utilized.

Researchers and policymakers in government will find this information valuable in their efforts to reduce the number of traffic fatalities (Abirami et al., 2021). ANN is used in the suggested method to prevent rear-end collisions and detect brake light from front vehicle. The vehicle speed, distance from the

16 more pages are available in the full version of this document, which may be purchased using the "Add to Cart" button on the publisher's webpage:

[www.igi-global.com/chapter/minimizing-data-loss-by-encrypting-brake-light-images-and-avoiding-rear-end-collisions-using-artificial-neural-network/340977](http://www.igi-global.com/chapter/minimizing-data-loss-by-encrypting-brake-light-images-and-avoiding-rear-end-collisions-using-artificial-neural-network/340977)

## Related Content

---

### Utilizations of AI in Cryptography: A Study

Meera S., Dinesh Kumar S., Sharmikha Sree R., Kalpana R. A. and Deepika R. (2024). *Machine Learning and Cryptographic Solutions for Data Protection and Network Security* (pp. 44-52).

[www.irma-international.org/chapter/utilizations-of-ai-in-cryptography/348601](http://www.irma-international.org/chapter/utilizations-of-ai-in-cryptography/348601)

### Blockchain Security Using Secure Multi-Party Computation

Jenila Livingston L. M., Ashutosh Satapathy, Agnel Livingston L. G. X. and Merlin Livingston L. M. (2021). *Opportunities and Challenges for Blockchain Technology in Autonomous Vehicles* (pp. 178-195).

[www.irma-international.org/chapter/blockchain-security-using-secure-multi-party-computation/262702](http://www.irma-international.org/chapter/blockchain-security-using-secure-multi-party-computation/262702)

### Quantum Computing for Cybersecurity: A Comparative Study of Classical and Quantum Techniques

Mohammad Alauthman, Ammar Almomani, Ahmad Al-Qerem, Mohammad A. Al Khaldy, Amjad Aldweesh, Ali Younis Al Maqousi and Mouhammd Alkasassbeh (2024). *Innovations in Modern Cryptography* (pp. 75-99).

[www.irma-international.org/chapter/quantum-computing-for-cybersecurity/354036](http://www.irma-international.org/chapter/quantum-computing-for-cybersecurity/354036)

### Supply Chain Governance Using DAO

Sujatha Gurunathan (2024). *Machine Learning and Cryptographic Solutions for Data Protection and Network Security* (pp. 444-456).

[www.irma-international.org/chapter/supply-chain-governance-using-dao/348623](http://www.irma-international.org/chapter/supply-chain-governance-using-dao/348623)

### An Area-Efficient Composite Field Inverter for Elliptic Curve Cryptosystems

M. M. Wong and M. L. D. Wong (2014). *Multidisciplinary Perspectives in Cryptology and Information Security* (pp. 218-237).

[www.irma-international.org/chapter/an-area-efficient-composite-field-inverter-for-elliptic-curve-cryptosystems/108032](http://www.irma-international.org/chapter/an-area-efficient-composite-field-inverter-for-elliptic-curve-cryptosystems/108032)