AIS Image Anomaly Detection of Ship Movement Using Convolutional Neural Network

Rose Hemans
Department for Decision Sciences
George Washington University
Washington, D.C.
rose.hemans@gwu.edu

Theodoros Pateros
Department for Decision Sciences
George Washington University
Washington, D.C.
tpateros@gwu.edu

***Abstract* - This paper presents a deep learning approach for detecting anomalous ship movements using images of Automatic Identification System (AIS) data. The approach utilizes a type of feed-forward neural network called a convolutional neural network (CNN) as an anomaly detection tool. Through transforming latitude and longitude coordinates into visual representations using Tableau, ship movement images were generated and used as input for the CNN. The methodology involved data preprocessing, image creation, and CNN training, resulting in a model adept at distinguishing normal from anomalous ship behaviors. The CNN exhibited robust classification abilities, effectively identifying irregular patterns within the AIS-derived images. This innovative fusion of CNNs with AIS data holds significant promise for enhancing maritime safety and traffic management. By enabling the early detection of potential safety risks through visual interpretations of AIS data, this approach offers a valuable tool for timely intervention in maritime scenarios. The study underscores the potential of utilizing CNNs in conjunction with AIS data to advance anomaly detection capabilities, emphasizing the importance of early anomaly identification for bolstering maritime navigation safety.**

I. Introduction

A. *Automatic Identification System (AIS) Data*

Against the backdrop of surging global ship traffic, anomalies in vessel movements represent a pressing concern for maritime safety and security. The Automatic Identification System (AIS), while pivotal for monitoring ship traffic, exhibits limitations in detecting covert activities, such as illicit ship-to-ship transfers or the transportation of oil from Russia post-Ukrainian conflict despite imposed sanctions. Anomalous behavior may also be related to pirate hijacking, maritime accidents, drug or human smuggling, or terrorist activities. These irregular movements not only raise concerns about compliance with international regulations but also signal potential safety hazards and nefarious actions. The evasion of sanctions and clandestine operations within maritime routes serves as a stark illustration of existing methods' inadequacies in capturing illicit or risky ship behaviors.

Many AIS datasets and databases of real-time traffic are freely available [1]. Shipping lanes and traffic density are shown in Figure 1 as a visualization example of AIS movement data in the Baltic Sea.

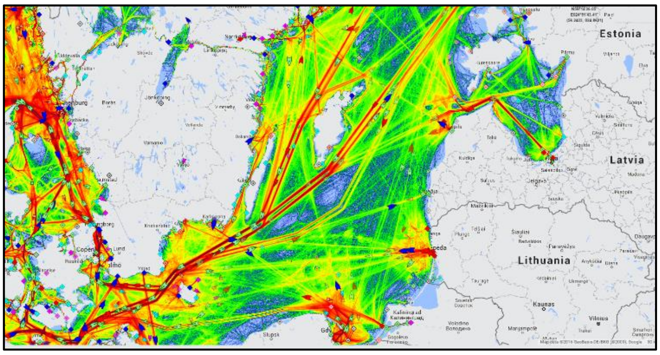


Fig 1: Visualization of AIS data in Baltic Sea. [2]

The motivation for our research lies in addressing these critical gaps by exploring alternative methods to complement AIS data. By acknowledging the limitations of tabular AIS data, our research aims to pioneer innovative approaches for anomaly detection. We seek to contribute to the enhancement of maritime safety protocols for the benefit of all stakeholders and the facilitation of more effective oversight and regulation within global maritime traffic. AIS information required to be transmitted covers static, dynamic, voyage, and safety-related features. Since this paper is focused on the simplification of anomaly detection of AIS tracks, we are most interested in the vessel's position (latitude and longitude) which are dynamic in order to plot AIS tracks for input data into our model.

TABLE I. SELECT AIS DATA FEATURES [1]

Name	Modeling Role	Description
MMSI	ID	Unique identifier
BaseDateTime	Plotting input	Time of receipt of AIS data
LAT	Plotting input	Latitude
LON	Plotting input	Longitude
Heading	excluded	Projected vessel course
VesselName	excluded	Name of vessel

B. *Anomaly Detection*

Anomaly detection, an integral facet across various domains, has a rich history rooted in statistical analysis and pattern recognition. Initially employed in diverse fields like finance, cybersecurity, and manufacturing, anomaly detection aimed to identify deviation from established norms or expected behavior. Traditional methods relied heavily on rule-based systems, statistical thresholds, or domain-specific heuristics to flag anomalies. However, the escalating complexities within datasets and emergence of diverse, intricate anomalies called for more adaptive and sophisticated approaches. Enter machine learning – a transformative force that revolutionized anomaly detection. Machine learning techniques, particularly unsupervised and semi-supervised algorithms, brought a paradigm shift by enabling systems to autonomously learn and discern anomalies from complex data patterns. With the advent of neural networks, especially deep learning architectures like Convolutional and Recurrent Neural Networks, anomaly detection gained unprecedented capabilities in deciphering intricate patterns and anomalies, even in high-dimensional and unstructured data. The fusion of machine learning with anomaly detection not only facilitated more accurate anomaly identification but also adapted to evolving anomalies, making it a cornerstone in modern anomaly detection methodologies across industries.

C. *Spoofing*

The maritime domain, once deemed relatively immune to cyber threats, has emerged as a vulnerable target for malicious actors due to its reliance on GPS and Automatic Identification System (AIS) technology. Spoofing, the act of manipulating these vital navigation and communication systems to provide false information, poses a significant and evolving threat to the safety, security, and economic integrity of global shipping. Understanding the motivations and ramifications of spoofing is crucial to mitigating its impact and safeguarding the maritime ecosystem. Monitoring of AIS data can identify spoofing cases amongst other applications for AIS anomaly detection. Further use cases AIS monitoring are listed in Table 2.

TABLE II. AIS MONITORING USE CASES

Activity Type	Activity
Criminal Activities	Drug trade/smuggling [3]
	Piracy [4]
	Cloaking vessel identity [3]
Environmental Monitoring	Overfishing [5]
	Illegal fishing [6]
Maritime Safety	Collision risks [7]
	Search and rescue [8]
	Traffic monitoring [9]

GPS spoofing involves transmitting forged signals that override a receiver's genuine positioning data. This can significantly alter the perceived location of a vessel, leading to disastrous consequences. Imagine a tanker deviating from its intended course due to spoofed GPS, potentially colliding with other ships or running aground on sensitive marine ecosystems. Beyond immediate navigational hazards, spoofed GPS can trigger false distress calls, diverting valuable rescue resources and disrupting emergency response protocols. Furthermore, automated navigation systems, increasingly prevalent on modern vessels, are susceptible to being manipulated by spoofed signals, compromising safety and potentially causing accidents.

AIS, mandated for most commercial vessels, broadcasts crucial information like a ship's identity, position, and course. Spoofing this data allows unscrupulous actors to mask their true intentions and activities. A seemingly harmless fishing vessel could morph into a stealthy pirate ship under the cloak of spoofed AIS, facilitating illegal activities like smuggling or resource extraction. Collisions become even more likely when genuine ship movements are obscured by spoofed AIS data, particularly in congested shipping lanes. Moreover, coastal authorities rely on accurate AIS information for traffic management and safety measures. Spoofing can disrupt these systems, creating navigational chaos and jeopardizing port operations.

The ramifications of spoofing extend far beyond isolated incidents of shipwrecks or pirate attacks. Disruptions to maritime traffic caused by spoofing-induced delays and accidents can trigger ripple effects throughout the global economy. Supply chains may become strained, leading to shortages and price hikes for essential goods. Damage to maritime infrastructure from spoofing-related collisions can cripple ports and pipelines, incurring significant repair costs and economic losses. Ultimately, the erosion of trust in maritime security due to spoofing incidents can deter investments and hinder the smooth flow of international trade.

Addressing the challenge of spoofing requires a coordinated and multifaceted approach. Technological advancements such as spoofing detection algorithms and more secure AIS protocols hold promise in deterring malicious actors. However, robust regulatory frameworks and stringent enforcement measures are equally essential to discourage spoofing activities and hold perpetrators accountable. Finally, raising awareness among maritime stakeholders about the risks of spoofing and best practices for prevention can serve as a crucial line of defense against this emerging threat.

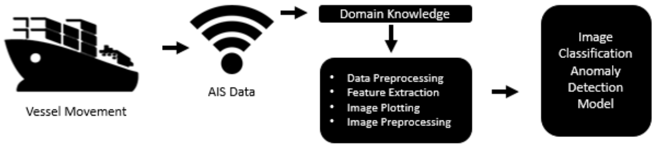


Fig 2: Example schematic of ship anomaly detection

II. RELATED WORK

A. Graph-Based Anomaly Detection Using CCTV Videos

Identifying abnormal behaviors in the complex network of maritime traffic is crucial for enhancing safety, security, and efficiency across global waterways. This section delves into the established field of anomaly detection within the maritime domain, specifically focusing on research exploring diverse data sources and computational approaches. The following properties of selected related studies are summarized in Table 1. Firstly, research methods are classified according to detection method. The publication author and year are listed then the studies are sorted by year and the detection method is noted.

TABLE III. DETECTION MODELS USED BY SELCT RECENT PRECEDING STUDIES

Detection Method	Publication		Detection Model
	Author	Year	
Statistical Analysis	Xiao [10]	2015	Statistical Distribution
	Rong et al. [4]	2019	Gaussian Process
Machine Learning	Vespe [7]	2012	Unsupervised Learning

Detection Method	Publication Author	 Year	Detection Model
Machine Learning	De Vries and van Someren [11]	2012	Clustering
	Toloue [12]	2019	Hidden Markov Model
	Zhang et al. [13]	2023	Clustering and Recurrent Neural network
Geometry	Zissis et al. [14]	2020	Spatial Method
	Guo et al. [15]	2021	Kinematic Interpolation
Prediction Based	Zhao [16]	2016	Long Short-Term Memory
	Singh and Heymann [6]	2020	Artificial Neural Network
	Seong et al. [17]	2023	Graph Convolutional Neural Network
	This Study	2023	Image Classification Convolutional Neural Network

Seong [17] explores the utility of CCTV video data and graph-based convolutional neural networks in identifying regular ship movements. Unlike traditional methods that rely on Automatic Identification System (AIS) data, this approach directly analyzes visual information, offering potential advantages in areas with limited AIS coverage or for detecting specific types of anomalies not captured by AIS data.

Seong uses CCTV video footage of maritime traffic as the primary data source. This data is segmented into individual ship tracks and converted into graphs representing the movements of ships over time. The model employs a Graph Convolutional Neural Network (GCNN) to learn normal ship movement patterns from the graph data. The GCNN can capture complex relationships and dependencies between different ships and their movements. The trained GCNN predicts the future trajectories of ships based on their past behavior. Deviations from these predicted trajectories are considered anomalies and flagged for further investigation (see Fig. 3).

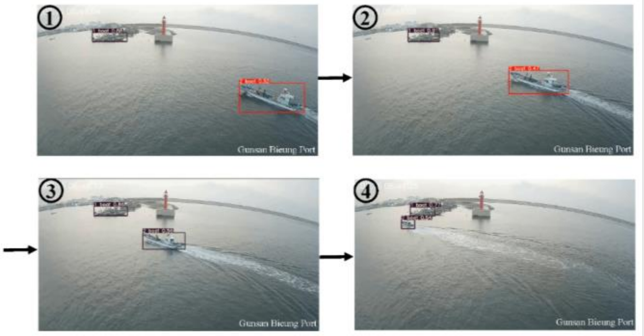


Fig. 3: Examples of abnormal movements in tracking results from Seong's research.

The authors evaluate their method on real-world CCTV video data, demonstrating its effectiveness in detecting various types of anomalous ship movements, such as:

- Unexpected changes in speed or direction
- U-turns or sudden stops
- Entering restricted areas
- Colliding with other vessels
- Loitering suspiciously

Advantages of the proposed method:

- **Directly analyzes visual information:** Can identify anomalies not captured by AIS data, such as sudden changes in course or collision avoidance maneuvers.
- **Applicable in areas with limited AIS coverage:** Useful for coastal areas, ports, and inland waterways where AIS coverage is often incomplete.
- **Provides visual evidence of anomalies:** CCTV footage can be used to confirm and investigate detected anomalies, aiding in decision-making and response.

Limitations of the method:

- **Requires access to CCTV data:** Installation and maintenance of CCTV cameras can be costly and impractical in all locations.
- **Susceptible to environmental factors:** Weather conditions and lighting can affect the quality of CCTV footage, potentially impacting the accuracy of anomaly detection.
- **Computationally expensive:** Training and running a GCNN requires significant computational resources.

B. Predicting Trajectories Using Bi-directional Gated Recurrent Unit (BiGRU)

Zhang [13] proposes a real-time method for detecting anomalous ship behavior using a combination of clustering and deep recurrent neural networks (DRNNs). It relies on Automatic Identification System (AIS) data, a widely available source of information on ship positions, headings, and speeds.

Zhang uses Density-Based Spatial Clustering of Applications with Noise (DBSCAN) identifies normal ship behavior patterns based on factors like location, speed, and heading. The algorithm is visualized in Fig. 4.

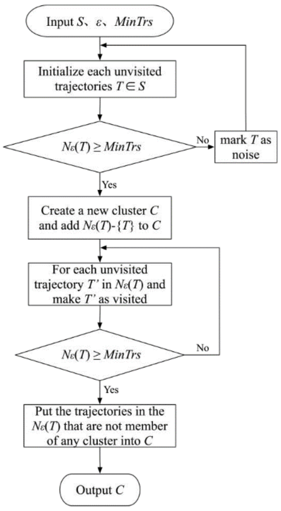

Input S、ε、$MinTrs$
Initialize each unvisited trajectories $T \in S$
$N_\varepsilon(T) \geq MinTrs$
No
mark T as noise
Yes
Create a new cluster C and add $N_\varepsilon(T)$-{T} to C
For each unvisited trajectory T' in $N_\varepsilon(T)$ and make T' as visited
$N_\varepsilon(T) \geq MinTrs$
No
Yes
Put the trajectories in the $N_\varepsilon(T)$ that are not member of any cluster into C
Output C

Fig. 4: DBSCAN-based ship trajectory clustering algorithm from Zhang's research.

This creates a model of what constitutes "normal" movement. A Bi-directional Gated Recurrent Unit (BiGRU) network, a type of DRNN, learns the temporal dynamics of these normal patterns within each cluster. Figure 5 depicts a schematic diagram of the BiGRU. Deviations from these learned patterns are flagged as anomalies. The research tests this method on real AIS data from the port of Tianjin, China. They report high accuracy and timeliness in detecting various anomalies, including deviations from regular routes, unexplained stops or changes in direction, exceeding speed limits, and entering restricted areas.

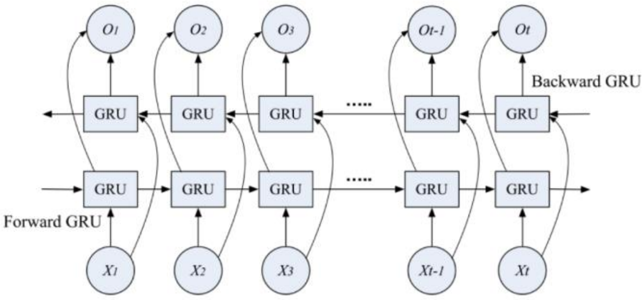


Fig. 5: Schematic diagram of Zhang's BiGRU for ship anomaly detection

Advantages of the proposed method:

- **Real-time detection:** Enables immediate identification of anomalies, allowing for swift intervention and response.
- **Cluster-based approach:** Adapts to different traffic patterns in specific areas, potentially improving accuracy compared to methods based on a single global model.
- **DRNN for temporal dynamics:** Captures the evolving nature of ship movements throughout their journeys, enhancing anomaly detection.

Limitations of the method:

- **Reliance on AIS data:** Accuracy depends on the availability and quality of AIS data, which can be unreliable in certain areas or for non-compliant vessels.
- **Model sensitivity:** Requires careful tuning of clustering and DRNN parameters to avoid overfitting or underfitting the data.
- **Computational complexity:** Training and running DRNNs can be computationally intensive, especially for large datasets.

C. 10 Year Review and Classifcation of Existing Approaches

Wolsing et al. [18] provide the most comprehensive review of recent approaches for anomaly detection in maritime Automatic Identification System (AIS) data. The review covers various anomaly detection techniques applied to AIS data, including statistical methods, machine learning algorithms, and deep learning models. Wolsing analyzes different approaches based on factors like accuracy, efficiency, adaptability, and robustness to noise or missing data.

According to the study, the main categories of methods have been statistical methods e.g., k-Nearest Neighbors, clustering, and outlier detection algorithms, Machine Learning e.g., Support Vector Machines and Random Forests, and Deep Learning where deep neural networks are utilized to learn complex patterns and relationships in AIS data without relying on handcrafted features. CNNs and RNNs are the most prominent examples.

Wolsing highlights the challenges of handling data quality issues, adapting to diverse traffic patterns, and incorporating additional data sources such as integrating visual information (CCTV) or environmental data (weather) to improve anomaly detection performance.

We believe our approach builds on existing methods and addresses some of the biggest challenges faced so far in the field. The use of image data reduces computational complexity, does not require access to CCTV cameras, and is not computationally expensive to train models on. Furthermore, images of AIS movement patterns are not susceptible to environmental factors since they are derived directly from AIS data and plotted using the Tableau data visualization software.

III. Proposed Approach/Method

A. Data Collection and Preparation

Our methodology revolves around leveraging Convolutional Neural Networks (CNNs) to detect anomalous ship movements using images derived from Automatic Identification System (AIS) data. To generate these images, latitude and longitude coordinates were transformed into visual representations employing Tableau. These visualizations served as the input data for the CNN.

B. Model Architecture

Figure 6 depicts a visualization of our model architecture. The core of our approach is a CNN architecture featuring sequential layers designed as follows:

Convolutional layers: The choice of three sets of convolutional layers was made to allow the network to learn increasingly complex patterns and features from the input data. Each set comprises convolutional layers followed by max-pooling layers, which helps in capturing hierarchical features while reducing spatial dimensions. The utilization of 64, 64, and 128 filters respectively indicates the depth or the number of unique features each layer aims to identify. A (3,3) kernel size signifies the window size used for feature extraction within the input data. The Rectified Linear Unit (ReLU) activation functions were applied to introduce non-linearity into the network, aiding in learning more intricate relationships within the data.

Flattening and dense layers: After the convolutional layers extract features, the resultant data is flattened into a single vector and fed into dense layers. This transformation allows the neural network to perform classification based on the learned features. The choice of a fully connected dense layer with 512 neurons and a ReLU activation function provides the network with the capacity to comprehend complex patterns within the extracted features. Incorporating a dropout of 0.5 within this layer aids in preventing overfitting by randomly dropping out half of the neurons during training, thereby enhancing the model's generalization capability.

Output layer: The final layer, comprising two neurons, utilizes a softmax activation function. This architecture suits the task of classifying ship behaviors into either normal or anomalous. The softmax function normalizes the output probabilities, providing a clear distinction between the two classes and enabling the model to make a decisive classification.

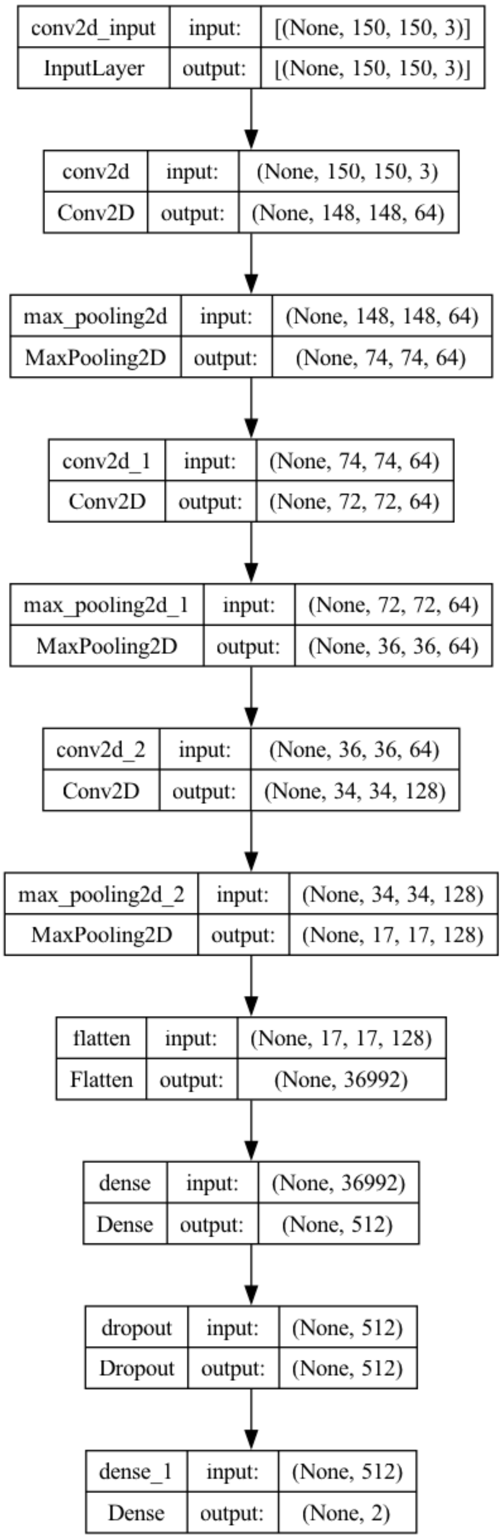

conv2d_input | input: | [(None, 150, 150, 3)]
InputLayer | output: | [(None, 150, 150, 3)]
conv2d | input: | (None, 150, 150, 3)
Conv2D | output: | (None, 148, 148, 64)
max_pooling2d | input: | (None, 148, 148, 64)
MaxPooling2D | output: | (None, 74, 74, 64)
conv2d_1 | input: | (None, 74, 74, 64)
Conv2D | output: | (None, 72, 72, 64)
max_pooling2d_1 | input: | (None, 72, 72, 64)
MaxPooling2D | output: | (None, 36, 36, 64)
conv2d_2 | input: | (None, 36, 36, 64)
Conv2D | output: | (None, 34, 34, 128)
max_pooling2d_2 | input: | (None, 34, 34, 128)
MaxPooling2D | output: | (None, 17, 17, 128)
flatten | input: | (None, 17, 17, 128)
Flatten | output: | (None, 36992)
dense | input: | (None, 36992)
Dense | output: | (None, 512)
dropout | input: | (None, 512)
Dropout | output: | (None, 512)
dense_1 | input: | (None, 512)
Dense | output: | (None, 2)

Fig. 6: Image Classification CNN Model Architecture

C. Model Training

Optimizer: The choice of the Adam optimizer is rooted in its adaptive learning rate methodology, which adjusts learning rates for each parameter individually. This adaptability leads to faster convergence and efficient gradient-based optimization. Adam is known for its effectiveness in handling large datasets and high-dimensional parameter spaces, making it a suitable choice for optimizing the model's weights and biases during training.

Loss Function: The sparse categorical cross-entropy loss function was selected for this classification task because it is well-suited for scenarios where there are two or more classes, and the classes are mutually exclusive. This loss function penalizes the model based on the difference between predicted and actual class probabilities, encouraging the model to correctly classify between normal and anomalous ship behaviors. The 'sparse' variant is employed when the classes are integers, allowing efficient computation by avoiding the need for one-hot encoding.

Training Parameters: Training the model over 15 epochs with a batch size of 10 suggests an iterative process where the entire dataset was divided in 10 batches and passed through the network 15 times. This balance between the number of epochs and batch size helps the model converge towards optimal weights and biases while minimizing computational resources. The choice of 15 epochs signifies a balance between model performance and training time, while a batch size of 10 strikes a balance between stochasticity in updating parameters and computational efficiency.

Resultant Model: The rigorous training process, characterized by the choice of optimizer, loss function, epochs, and batch size, has led to a proficient model. This model demonstrates a high level of effectiveness in accurately distinguishing between normal and anomalous ship behaviors within the AIS-derived images. The combination of these training parameters contributes significantly to the model's capability to generalize well and make accurate predictions on unseen data.

IV. System Design and Implementation

A. Architecture Overview

The implemented system represents a robust fusion of CNNs with AIS data, serving as a pioneering tool for detecting irregular ship movements. This amalgamation capitalizes on the CNN's adeptness in discerning intricate patterns within AIS-derived visualizations.

B. Datasets

Our meticulously curated dataset, derived from real-world vessel trajectories, encompasses labeled instances categorizing normal and suspicious ship activities. This comprehensive dataset serves as the cornerstone for training and validating the CNN model.

C. Major Components

Vessel trajectory data was processed using Tableau to create visual representations serving as input for the CNN, forming the basis for anomaly detection. The core of the system, the CNN model, underwent rigorous training using the labeled dataset, equipping it to identify abnormal ship behaviors within AIS-derived images.

V. Model Evaluation

Figure 7 visualizes the training and validation accuracy and loss of the model. The model performance was assessed based on its training and validation metrics across 15 epochs:

Loss and Accuracy Trends: The training process shows a progressive decrease in the loss function, indicating that the model steadily improved in minimizing errors concerning the training data. Simultaneously, the accuracy metric demonstrates an increasing trend, signifying the model's growing ability to correctly classify ship movements within the training dataset.

Validation Metrics – Accuracy: The validation accuracy fluctuated across epochs, oscillating between approximately 62% and 93%. This fluctuation could indicate occasional overfitting or sensitivity to the validation dataset.

Validation Metrics – Loss: The validation loss exhibited a downward trend initially, reaching a minimum around epoch 10, suggesting that the model's generalization to unseen data improved progressively.

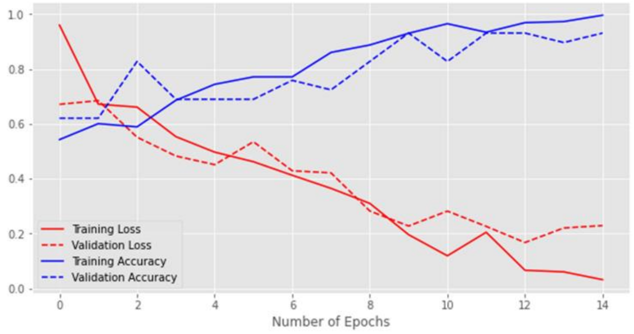


Fig. 7: Image Classification CNN Training/Validation Loss and Accuracy

Overfitting Consideration: The model showcased signs of potential overfitting during the initial epochs, as indicated by the gap between the training and validation accuracies. However, this gap gradually diminished, aligning more closely between epochs 10 and 15, suggesting improved generalization.

Accuracy Analysis: The model achieved promising results in terms of accuracy, with peak validation accuracy reaching approximately 93%. This denotes the model's ability to correctly classify normal and anomalous ship behaviors in the unseen validation dataset. A small test set was split from the original data and Figure 8 depicts a confusion matrix of the model's performance on this unseen test set.

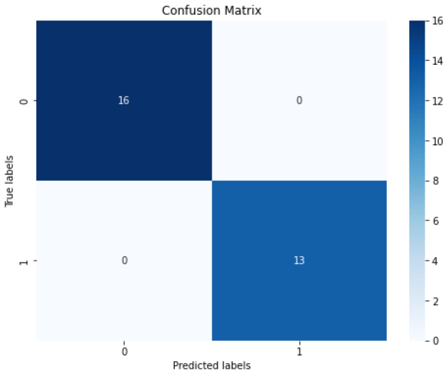
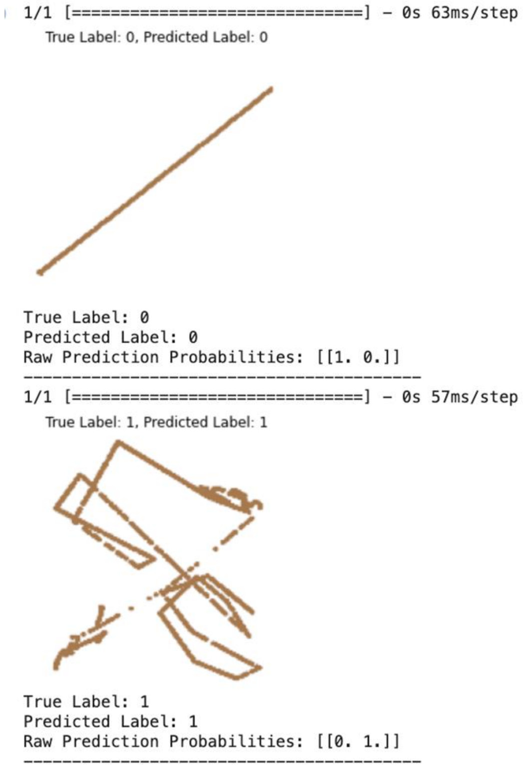


Fig. 8: CNN test set confusion matrix

Loss Analysis: The validation loss, consistently decreasing for the initial epochs, indicated effective learning and minimized errors on the validation data. However, a slight increase in loss during later epochs may warrant further investigation to ensure continued model improvement.

Epoch-wise Observations: The most significant performance enhancements were observed between epochs 1 to 10, with accuracy notably improving and loss steadily decreasing. Beyond epoch 10, the model's improvements became more marginal, suggesting a convergence towards an optimal performance level. An example of the model's prediction capabilities can be seen in Figure 9.



```
1/1 [==============================] - 0s 63ms/step
   True Label: 0, Predicted Label: 0

True Label: 0
Predicted Label: 0
Raw Prediction Probabilities: [[1. 0.]]
----------------------------------------
1/1 [==============================] - 0s 57ms/step
   True Label: 1, Predicted Label: 1

True Label: 1
Predicted Label: 1
Raw Prediction Probabilities: [[0. 1.]]
----------------------------------------
```

Fig. 9: CNN Image Prediction

VI. Discussion and Conclusion

This study presents a pioneering approach that leverages Convolutional Neural Networks (CNNs) for the early detection of anomalous ship movements using images derived from Automatic Identification System (AIS) data. By transforming latitude and longitude coordinates into visual representations via Tableau, this innovative fusion of CNNs and AIS data offers a promising tool for maritime anomaly detection.

The methodology involved data preprocessing, image creation, and CNN training, culminating in a model adept at discerning normal from anomalous ship behaviors. The CNN exhibited robust classification abilities, effectively identifying irregular patterns within AIS-derived images, thus addressing critical gaps in traditional AIS-based anomaly detection systems.

The motivation behind this research stemmed from recognizing the limitations of tabular AIS data in capturing covert or risky ship behaviors, which pose substantial safety, security, and economic risks in global maritime traffic. Anomalies, spanning from illicit activities like smuggling to potential hazards such as pirate hijacking or accidents, underscore the need for advanced anomaly detection methodologies.

Our study builds upon the foundations laid by existing anomaly detection techniques within the maritime domain. We aimed to pioneer an approach that harnesses the power of CNNs while circumventing challenges associated with traditional methods, such as reliance on limited data sources or computational complexity.

Spoofing emerged as a critical concern in maritime security due to its potential to manipulate GPS and AIS technologies, posing threats ranging from navigational hazards to economic disruptions. Understanding these challenges is vital in developing robust mitigation strategies that incorporate technological advancements, regulatory frameworks, and stakeholder awareness. In comparing our approach with existing techniques, the use of image data derived directly from AIS provides a computationally efficient, reliable, and accessible means of anomaly detection. While acknowledging the strengths of methods like CCTV-based anomaly detection or clustering with deep recurrent networks using AIS data, our approach presents a distinctive solution that is less reliant on additional infrastructure and more adaptable to various maritime scenarios.

The CNN model's architecture, comprising convolutional layers, dense layers, and a softmax output layer, facilitated accurate classification of ship behaviors into normal and anomalous categories. The training process, optimized through parameters like the Adam optimizer, sparse categorical cross-entropy loss function, and epoch-batch size balance, resulted in a proficient model capable of generalizing well to unseen data. The model's performance evaluation across 15 epochs revealed a trend of increasing accuracy and decreasing loss, showcasing its capability to accurately discern ship behaviors. Though occasional fluctuations and signs of early overfitting were observed, the convergence of training and validation metrics toward the latter epochs indicated improved generalization.

This study's contributions extend to bolstering maritime safety protocols, fostering effective traffic management, and offering a valuable intervention tool for potential safety risks. It emphasizes the pivotal role of CNNs in enhancing anomaly detection within AIS data, thus affirming the significance of early anomaly identification in fortifying maritime navigation safety.

Moving forward, further exploration into fine-tuning the model beyond epoch 10 and extensive testing across diverse anomalies will be instrumental in fortifying the model's robustness in real-world maritime scenarios. The implications of this research underscore the potential of CNNs in revolutionizing anomaly detection within AIS data and highlight technology's critical role in ensuring safer and more secure maritime navigation. This work serves as a foundational step towards deploying innovative AI-driven solutions in the maritime domain, emphasizing the potential of CNNs to revolutionize anomaly detection methodologies and underlining the importance of early anomaly identification for fortified maritime navigation safety.

Acknowledgment

Conceptualization, T.P, R.H.; methodology, T.P., R.H.; data curation, T.P.; software, T.P., writing – original draft preparation, R.H., T.P., writing - review and editing, R.H., T.P.

References

[1] “Nationwide Automatic Identification System 2015 | InPort,” *www.fisheries.noaa.gov*. https://www.fisheries.noaa.gov/inport/item/52805 (accessed Dec. 16, 2023).

[2] J. Davis, “BALTIC SEA AIS Ship Traffic Live Map | Marine Vessel Traffic,” www.marinevesseltraffic.com, Dec. 16, 2023. https://www.marinevesseltraffic.com/BALTIC-SEA-AIS/ship-traffic-trackerSeong, N.; Kim, J.; Lim, S. Graph-Based Anomaly Detection of Ship Movements Using CCTV Videos. J. Mar. Sci. Eng. 2023, 11, 1956. https://doi.org/10.3390/ jmse11101956

[3] M. Balduzzi, A. Pasta, and K. Wilhoit, “A security evaluation of AIS automated identification system,” Proceedings of the 30th Annual Computer Security Applications Conference, Dec. 2014, doi: https://doi.org/10.1145/2664243.2664257.

[4] H. Rong, A. P. Teixeira, and C. Guedes Soares, “Data mining approach to shipping route characterization and anomaly detection based on AIS data,” Ocean Engineering, vol. 198, p. 106936, Feb. 2020, doi: https://doi.org/10.1016/j.oceaneng.2020.106936.

[5] F. Natale, M. Gibin, A. Alessandrini, M. Vespe, and A. Paulrud, “Mapping Fishing Effort through AIS Data,” PLOS ONE, vol. 10, no. 6, p. e0130746, Jun. 2015, doi: https://doi.org/10.1371/journal.pone.0130746.

[6] S. K. Singh, “Machine Learning-Assisted Anomaly Detection in Maritime Navigation using AIS Data | IEEE Conference Publication | IEEE Xplore,” ieeexplore.ieee.org, Apr. 23, 2020. https://ieeexplore.ieee.org/abstract/document/9109806

[7] M. Vespe, I. Visentini, K. Bryan and P. Braca, "Unsupervised learning of maritime traffic patterns for anomaly detection," 9th IET Data Fusion & Target Tracking Conference (DF&TT 2012): Algorithms & Applications, London, 2012, pp. 1-5, doi: 10.1049/cp.2012.0414.

[8] I. Varlamis, “Detecting Search and Rescue Missions from AIS Data | IEEE Conference Publication | IEEE Xplore,” ieeexplore.ieee.org, 2018. https://ieeexplore.ieee.org/document/8402020 (accessed Dec. 16, 2023).

[9] M. Gao, G. Shi, and S. Li, “Online Prediction of Ship Behavior with Automatic Identification System Sensor Data Using Bidirectional Long Short-Term Memory Recurrent Neural Network,” Sensors, vol. 18, no. 12, p. 4211, Nov. 2018, doi: https://doi.org/10.3390/s18124211.

[10] F. Xiao, H. Ligteringen, C. van Gulijk, and B. Ale, “Comparison study on AIS data of ship traffic behavior,” *Ocean Engineering*, vol. 95, pp. 84–93, Feb. 2015, doi: https://doi.org/10.1016/j.oceaneng.2014.11.020.

[11] De Vries, G.K.D. and Van Someren, M., 2012. Machine learning for vessel trajectories using compression, alignments and domain knowledge. Expert Systems with Applications, 39(18), pp.13426-13439.

[12] Toloue, K.F. and Jahan, M.V., 2018, February. Anomalous behavior detection of marine vessels based on Hidden Markov Model. In 2018 6th Iranian Joint Congress on Fuzzy and Intelligent Systems (CFIS) (pp. 10-12). IEEE.

[13] Zhang, B.; Hirayama, K.; Ren, H.; Wang, D.; Li, H. Ship Anomalous Behavior Detection Using Clustering and Deep Recurrent Neural Network. J. Mar. Sci. Eng. 2023, 11, 763. https://doi.org/ 10.3390/jmse11040763

[14] Zissis, D., Chatzikokolakis, K., Spiliopoulos, G. and Vodas, M., 2020. A distributed spatial method for modeling maritime routes. IEEE Access, 8, pp.47556-47568.

[15] Guo, S., Mou, J., Chen, L. and Chen, P., 2021. An anomaly detection method for AIS trajectory based on kinematic interpolation. Journal of Marine Science and Engineering, 9(6), p.609.

[16] Zhao, L. and Shi, G., 2019. Maritime anomaly detection using density-based clustering and recurrent neural network. The Journal of Navigation, 72(4), pp.894-916.

[17] Seong N, Kim J, Lim S. Graph-Based Anomaly Detection of Ship Movements Using CCTV Videos. Journal of Marine Science and Engineering. 2023; 11(10):1956. https://doi.org/10.3390/jmse11101956

[18] Wolsing, K.; Roepert, L.; Bauer, J.; Wehrle, K. Anomaly Detection in Maritime AIS Tracks: A Review of Recent Approaches. J. Mar. Sci. Eng. 2022, 10, 112. https:// doi.org/10.3390/jmse10010112