Faculty of Natural and Applied Sciences Journal of Computing and Applications
Print ISSN: 3026-8133
www.fnasjournals.com
Volume 2; Issue 3; May 2025; Page No. 52-61.
DOI: https://doi.org/10.63561/jca.v2i3.836

Leveraging on Hybridized CNN- HARS Surveillance Model for Security Threat detection in Imo State, Nigeria

[*]Ohanaka, B. U., Michael, O. D., Udeogu C., Bardi, I. A., & Odoemene, I. O.
Department of Computer Science, Alvan Ikoku Federal University of Education, Owerri.

***Corresponding author email:** bethrand.ohanaka@alvanikoku.edu.ng

Abstract

The escalating security threats in Imo State, including terrorism, unknown gunmen attacks, kidnapping, one-chance drivers, and armed robbery, have created an urgent need for effective surveillance solutions. This study presents an integrated Convolutional Neural Network (CNN) and Human Activity Recognition System (HARS) model to enhance real-time security surveillance. Video feeds from strategically deployed CCTV cameras and drones are processed through a CNN for spatial feature extraction, identifying critical elements like edges, textures, and human shapes. Features indicative of suspicious behaviours, such as loitering or carrying weapons, are refined using Rectified Linear Unit (ReLU) activation functions and downsampled via pooling. Flattening and fully connected layers classify activities into normal (0.0–0.3), suspicious (0.4–0.6), or threat (0.7–1.0) categories. The HARS component complements CNN by performing temporal analysis, recognising activity patterns that may escalate into criminal behaviour. The system triggers real-time alerts for suspicious and threat activities, enabling rapid responses from security agencies. The model was evaluated on a 500-sample label dataset, achieving an accuracy of 84%, a precision of 86.96%, a recall of 80%, and an F1-score of 83.3%, demonstrating its capability to detect and classify security threats effectively. The findings highlight the transformative potential of advanced surveillance systems in improving public safety, aiding law enforcement, and restoring stability in Imo State. This innovative approach provides a robust tool for combating crime and enhancing security in both urban and remote areas.

Keywords: Security surveillance, Convolutional Neural Network, Human Activity Recognition System, real-time detection, artificial intelligence, deep learning, crime prevention.

Introduction

The escalating waves of insecurity in Nigeria have affected many states in the eastern region and the country at large, with Imo State as one of the most negatively affected in the socio-economic well-being and political stability of the state. Unemployment, poverty, porous borders, corruption, internet fraud of all kinds, among others, have contributed to the state of insecurity and increased crime rate in the country, leaving unpalatable challenges for the nation's economy and its growth (Achumba et al., 2013). Recently, Imo state has witnessed rise in violent crimes, such as terrorism, unknown gunmen, armed robberies, kidnappings for ransom, activities of one chance drivers, which have cause fear to the citizens and a great concern for both the government and security agencies. Insecurity in Imo State can be linked to both internal and external factors, including the unresolved political issues, political tensions surrounding the Biafra movement, which have on many occasions led to violent confrontations between security forces and insurgent groups. According to Okafor and Udo (2021), the demand for secession from the Indigenous People of Biafra (IPOB) has further strained the fuel insecurity, thereby straining the stability of the eastern region and hindering effective governance. Although several efforts have been made to tackle this and many more security threats, Omenga (2013) opined that despite several efforts made to tackle security challenges lack of quick response from the Nigeria Police Force during crime time is one of the lapses in fighting insecurity. According to Omenga, some analysts have opined that perhaps the government or some groups of unscrupulous government officials have been using the unknown gunmen saga as a gambit for political gain.

The disturbing security situation has made Imo state government to adopt many security strategies, by increasing the number of Police and Military men deployed along the major roads, villages and strategic locations in the state, which have created a stop and search checkpoint, conducting patrols, gathering intelligence information of criminal activities to combat these crimes. The use of technology, including closed-circuit television (CCTV) surveillance and the installation of monitoring systems in key areas, has also been incorporated into the state's security framework. CCTV cameras are installed in some local government, urban centres, roads, and other vulnerable locations to help monitor criminal activities.

However, despite these efforts, there is still a growing influence of criminal activities and insurgent groups within the state as the current security surveillance system has not been able to mitigate effectively, which can be attributed to the lack of real-time data processing and response capability. For example, many of the CCTV systems in place are often poorly maintained and lack the capacity to cover the entire state or provide high-resolution images that can aid in the identification of criminals. Furthermore, the security forces' reliance on traditional methods of crime detection, such as physical patrols and intelligence gathering through human sources, limits their ability to track and anticipate the movements of criminal elements.

The rapid evolution of crime in the state, particularly with the rise of armed insurgency and organised criminal syndicates, has outpaced the capabilities of the existing surveillance infrastructure. The adoption of an AI-driven surveillance system, HARS-CNN technique, to monitor, detect and report suspected criminal activities in real-time will present an effective solution to security challenges ravaging Imo state. Leveraging the ability of CNNs to extract complex patterns from video feeds from drones and CCTV cameras to identify weapons, and track individuals engaged in criminal activities in real-time, and HARS in analyzing human activities such as carrying weapons, kidnapping, loitering, robbery, struggling and fighting detect suspicious behaviors, will enhance the capacity of security framework to monitor and report security threat to foster a proactive measure for crime prevention in Imo state. This study, therefore, seeks to explore the development and deployment of an AI-enhanced surveillance framework using HARS-CNN to strengthen security monitoring, threat detection, and proactive crime response in Imo State.

Convolutional Neural Networks (CNN)

Convolutional Neural Networks (CNNs) are a specialised class of deep learning models designed for processing and analysing data with a grid-like topology, such as images, video frames, or spatial data. Introduced by LeCun et al. (1998), CNNs have become foundational in modern computer vision tasks due to their ability to automatically and hierarchically learn spatial features from input data. CNNs are widely regarded for their exceptional performance in image recognition and classification tasks, making them a core component of intelligent video surveillance systems (Krizhevsky et al., 2012). They automatically extract hierarchical features from raw image data using convolutional and pooling operations, which is particularly effective in detecting specific objects such as guns, knives, and suspicious packages in crowded environments. Redmon et al. (2016) introduced the YOLO (You Only Look Once) model, a real-time object detection system that has since been used extensively in surveillance to detect multiple objects in a single frame. Similarly, Faster R-CNN (Ren et al., 2015) and SSD (Single Shot MultiBox Detector) (Liu et al., 2016) have been applied to identify unusual activities and provide real-time alerts. These models outperform traditional surveillance methods by reducing response times and minimising false alarms.

The CNN architecture, as shown in Figure 1**,** is structured in a layered manner, consists of an input layer, convolutional layers, pooling layers, and fully connected layers.

Input layer: This is the first layer that receives the raw input data. It typically consists of a multidimensional array that represents the data, such as an image with width, height, and colour channels. The input layer does not perform any computations but simply passes the data to the next layer. It essentially serves as the gateway through which the

Cite this article as:
Ohanaka, B. U., Michael, O. D., Udeogu C., Bardi, I. A., & Odoemene,I. O. (2025). Leveraging a hybridized CNN-HARS surveillance model for security threat detection in Imo State, Nigeria. *FNAS Journal of Computing and Applications, 2*(3), 52-61. https://doi.org/10.63561/jca.v2i3.836

data enters the network. The structure of the input layer depends on the format and dimensions of the data, and it must match the expected input size for the CNN model.

Convolutional Layers: They are the cornerstone of CNNs, where kernels (filters) slide across the input data to extract local features like edges, corners, or textures. These layers exploit spatial hierarchies by focusing on localised patterns in the input, which are critical for image and video data analysis (Krizhevsky et al., 2012). Each kernel's weights are learned during training, allowing the model to adapt to specific features relevant to the task.

Pooling Layers: It reduces the spatial dimensions of feature maps while retaining essential information, making the computation more efficient and mitigating overfitting. Common pooling techniques include max pooling, which selects the highest value in a local region, and average pooling, which computes the average (Goodfellow et al., 2016).

Fully Connected Layers: They serve as the final stage of the CNN, where the learned spatial features are mapped to output predictions. These layers treat the high-level features from convolutional layers as input and connect them to the specific classes or outputs of the model.

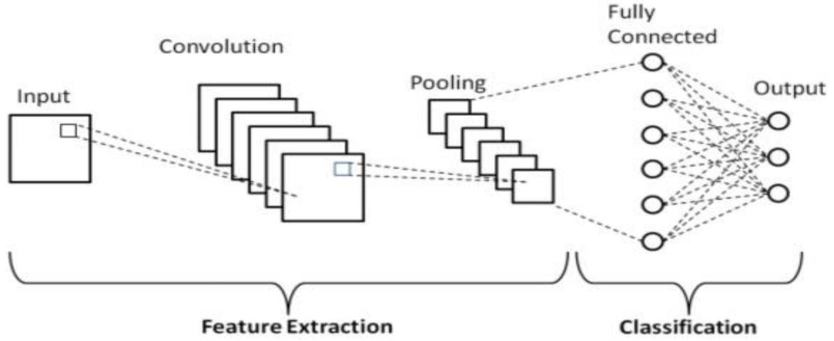
Activation Functions: They are applied to introduce non-linearity, allowing the CNN to learn complex patterns. Rectified Linear Unit (ReLU) has become a standard in CNNs due to its simplicity and ability to mitigate the vanishing gradient problem (Glorot et al., 2011).

Training: The training of CNNs involves optimising the weights of kernels and fully connected layers through backpropagation. A loss function, such as cross-entropy for classification tasks, quantifies the difference between predicted outputs and actual labels. The optimisation process, typically driven by algorithms like Stochastic Gradient Descent (SGD) or Adam, minimises this loss by iteratively updating weights (Kingma & Ba, 2015).

To improve generalisation, techniques like data augmentation and dropout are often employed. **Data augmentation** artificially increases the diversity of the training dataset by applying transformations such as rotation, flipping, and scaling.

Dropout, on the other hand, randomly disables neurons during training, reducing the risk of over-fitting (Srivastava et al., 2014).

Figure 1
CNN Architecture



Source: https://medium.com/thedeephub/convolutional-neural-networks-a-comprehensive-guide-5cc0b5eae175

Human Activity Recognition System (HARS)

Human Activity Recognition (HARS) is the process of interpreting human actions through sensors or visual input. HARS uses AI and computer vision algorithms to identify behaviours like walking, running, loitering, fighting, or carrying weapons, activities that may be precursors to crimes (Lara & Labrador, 2013). These systems often utilise

Cite this article as:
Ohanaka, B. U., Michael, O. D., Udeogu C., Bardi, I. A., & Odoemene,I. O. (2025). Leveraging a hybridized CNN-HARS surveillance model for security threat detection in Imo State, Nigeria. *FNAS Journal of Computing and Applications, 2*(3), 52-61. https://doi.org/10.63561/jca.v2i3.836

deep learning techniques such as CNNs, LSTMs, and 3D Convolutional Networks to model temporal and spatial patterns from video sequences (Wang et al., 2018). HAR models have also been applied in sensitive environments like airports, banks, and shopping malls to preemptively alert security personnel of potential threats. The integration of HARS into drone-based surveillance has further improved area coverage and activity tracking in military and disaster zones (Kim et al., 2019).

These systems rely on data gathered from high-resolution cameras or other imaging devices, which capture continuous streams of footage. Once the data is captured, it is processed using sophisticated algorithms that classify the human activity in real-time (Zhang et al., 2021). HARS' major strength lies in its ability to distinguish between ordinary and abnormal behaviours. By using predefined models that represent typical activities, HARS can flag activities that deviate from these models. This includes identifying individuals who exhibit suspicious movements, such as rapidly moving through an area or engaging in behaviours that are inconsistent with normal daily patterns. Furthermore, HARS systems are often designed to operate in real-time, making them ideal for dynamic environments like public spaces or remote areas. One significant advantage of HARS is their ability to integrate with other technologies, such as drones or surveillance networks, offering broader coverage in monitoring remote or expansive areas. These systems can also be enhanced by incorporating facial recognition capabilities, which can aid in identifying criminals or individuals of interest during surveillance operations (Zhu et al., 2020).

Despite these potentials of HARS, there are some challenges in implementing and deploying it in a real-world environment. One challenge is the need for large, labelled datasets for training machine learning models, as accuracy depends on the variety and quality of data used in the training phase. Moreover, ensuring the robustness of these systems in detecting behaviours under varying environmental conditions, such as different lighting or weather conditions, can be complex (Cheng et al., 2019). Despite these hurdles, advancements in deep learning and data augmentation techniques continue to improve the efficacy of HAR, making it increasingly reliable in security applications.

The next section presents the aim and objectives of the study as well as the key challenges this research aims to address.

Aim and objectives

This study aims to develop an intelligent real-time security surveillance system by integrating Convolutional Neural Networks (CNN) with a Human Activity Recognition System (HARS) to improve the detection, classification, monitoring, and reporting of criminal activities in Imo state. The specific objectives of the study are:

1. To detect and classify dangerous objects such as firearms and explosives in real-time using a CNN from video feeds captured by CCTV cameras and drones.
2. To analyse human activities (e.g., loitering, fleeing, or carrying suspicious items) using the Human Activity Recognition System (HARS).
3. To develop a hybrid CNN-HARS surveillance model for real-time threat detection, alert generation, and automatic notification to security agencies.
4. To analyse historical crime pattern data that identifies high-risk hotspots and facilitates proactive security planning and resource allocation.

Security challenges in Imo state

The security challenges facing Imo state can be identified but not limited to terrorism, activities of Unknown gunmen, kidnapping for ransom, armed robbery, one chance drivers and others. The weak surveillance systems have threatened the social stability, economic growth and public safety of the people of the state, which calls for urgent technology-driven solutions for lasting peace and improved security.

a. **Terrorism and Insurgency**: Imo State has witnessed the rise of terrorism and insurgent activities, particularly linked to the Indigenous People of Biafra (IPOB) and its militant arm, the Eastern Security Network (ESN). These groups have escalated their attacks on government officials, security forces, and civilians, and unlawfully impose a sit-at-home order on Mondays. They engage in guerrilla tactics, such as ambushes, assassinations, and bombings,

Cite this article as:
Ohanaka, B. U., Michael, O. D., Udeogu C., Bardi, I. A., & Odoemene,I. O. (2025). Leveraging a hybridized CNN-HARS surveillance model for security threat detection in Imo State, Nigeria. *FNAS Journal of Computing and Applications, 2*(3), 52-61. https://doi.org/10.63561/jca.v2i3.836

targeting both security forces and critical infrastructure. These insurgent activities are part of a broader struggle for Biafran independence, with armed confrontations frequently resulting in loss of life and property. The increasing frequency of such violent acts is destabilising the region, undermining both state authority and public trust in law enforcement

b. **Activities of Unknown Gunmen**: The term “unknown gunmen” is used to describe individuals or groups that operate under anonymity and engage in violent crimes. These groups often operate in small but heavily armed cells, targeting security forces, political figures, and civilians. The rise of unknown gunmen has been particularly alarming, as these groups use hit-and-run tactics, ambushing security forces at checkpoints and causing fear among residents. The state has witnessed an increase in the activities of unknown gunmen who target security personnel, government infrastructure, and civilians. These perpetrators, often operating from hidden locations such as bushes, valleys, and caves, execute ambush-style attacks, creating widespread fear and destabilization in communities (Eze & Uka, 2023). This shadowy nature of the gunmen makes them difficult to track, with the lack of intelligence and community support contributing to their continued presence. Recent attacks, such as those in Okigwe and parts of Owerri, have left several police officers and civilians dead.

c. **Kidnapping for Ransom**: Kidnapping for ransom is another prevalent security challenge in Imo state. People are abducted while traveling, while entering their houses or other area in broad daylight, in most cases at night and taken to secluded areas where negotiations for ransom payments take place between the victims’ family members and the kidnappers. The financial and psychological toll on families and communities cannot be underestimated, necessitating proactive and intelligent surveillance solutions (Oketa, 2018). Kidnapping for ransom has become an increasingly prevalent crime in Imo State, as criminal groups target rich businessmen, people that come back from abroad, top government officials and high-profile individuals in society for financial gain. Victims, ranging from politicians to business owners and ordinary citizens, are abducted and held hostage until a ransom is paid. The proliferation of firearms has worsened the rate, making it easier for criminals to carry out kidnappings. Additionally, the high levels of poverty and unemployment in the region have fueled criminal activities like kidnapping. A growing number of syndicates have emerged, often well-organised and sophisticated in their methods, leading to a climate of fear that has affected both residents and visitors to the state

d. **One Chance Drivers**: The term "one-chance drivers" refers to criminals disguising themselves as legitimate commercial transport drivers who lure unsuspecting passengers inside their vehicles and often take them to hidden locations where they are dispossessed of their valuables at gunpoint and, in some cases, harmed. Amid the myriad of security challenges bedevilling Nigeria, one-chance robberies seem to have become a part of the daily existence of citizens. One minute your phone is in your bag, and the next, it’s no longer there (Abimbola, 2024).

The activities of "one chance drivers" are another significant security concern in Imo, which has been linked to the breakdown of law enforcement in the state, as these criminal groups have found it easy to operate with minimal interference. The anonymity provided by public transport vehicles and the lack of stringent regulatory oversight have made this form of robbery highly effective, with many residents wary of using public transport for fear of being targeted

. **Armed Robbery**: Criminal gangs, often heavily armed with firearms and other weapons, target individuals and businesses, sometimes leading to violent confrontations. These robberies have been described as violent and opportunistic, with robbers engaging in shootouts with police forces or stealing from shops and homes. According to Otuu et al. (2022), armed robbery incidents in Imo State, particularly in residential areas, banks, rural regions, and along major highways, remain a persistent threat. Perpetrators often operate in groups, using sophisticated weapons to execute their crimes. The lack of effective monitoring systems contributes to the high success rate of such criminal activities. The increasing number of armed robbers has been linked to the proliferation of small arms in the region, exacerbated by the political instability and insurgency activities (Adeleke et al., 2022). Moreover, some armed robbers are believed to have connections with terrorist groups, further complicating the law enforcement response.

Methodology

The development of an integrated Convolutional Neural Network (CNN) and Human Activity Recognition Systems (HARS) model for enhanced security surveillance is a multi-stage process that combines spatial and temporal analysis to detect, classify, and respond to activities in real time. This comprehensive system processes video feeds

Cite this article as:
Ohanaka, B. U., Michael, O. D., Udeogu C., Bardi, I. A., & Odoemene,I. O. (2025). Leveraging a hybridized CNN-HARS surveillance model for security threat detection in Imo State, Nigeria. *FNAS Journal of Computing and Applications, 2*(3), 52-61. https://doi.org/10.63561/jca.v2i3.836

from CCTV cameras and drones placed in key urban and remote areas, ensuring accurate detection of criminal activities and timely responses.

Input Layer and Preprocessing: The process begins at the input layer, where video frames are digitised and standardised to ensure uniformity in processing. The system preprocesses the video by extracting individual frames, resizing them to the required input dimensions (e.g., 224x224 pixels), normalising pixel values, and performing data augmentation to enhance diversity. This ensures the model is robust and can handle variations in lighting, angles, and environmental conditions.

CNN Stages (Spatial Feature Extraction): In the first phase, the CNN component conducts spatial analysis. Convolutional layers apply filters or kernels across the input frames, computing feature maps that capture important spatial features like edges, textures, and human shapes. This enables the system to identify patterns such as loitering, running, or carrying suspicious objects.

The extracted feature maps are passed through Rectified Linear Unit (ReLU) activation functions, which remove irrelevant negative values and focus computational resources on significant features, such as the outline of a weapon or unusual postures. Next, pooling layers like max pooling downsample the feature maps, reducing spatial dimensions while retaining essential details. This process lowers computational requirements and ensures that critical features, such as the presence of a weapon or abnormal movements, are preserved.

The output from the pooling stage is passed to the flatten layer, which converts the multi-dimensional feature maps into a one-dimensional vector. This vector bridges the feature extraction stages and the classification phase.

Fully Connected Layer and Classification: The fully connected layer processes the flattened vector, linking the extracted features to predefined activity categories. Dense connections in this layer enable the model to understand relationships between features, classifying activities into three categories: Normal (0.0–0.3), Suspicious (0.4–0.6), or Threat (0.7–1.0). The final classification uses a softmax activation function, which outputs a probability distribution over these categories. For example, the model may classify a person running with a suspicious object as a "Threat" with a high probability.

HARS Integration (Temporal Analysis): The classified output from CNN is then passed to the HARS component for temporal analysis. HARS uses techniques like Long Short-Term Memory (LSTM) networks or Temporal Convolutional Networks (TCNs) to analyse sequential patterns across frames. This temporal analysis detects ongoing activities, such as extended loitering or repetitive movements that may indicate criminal behaviour. By combining CNN's spatial insights with HARS's temporal analysis, the system achieves a comprehensive understanding of activities.

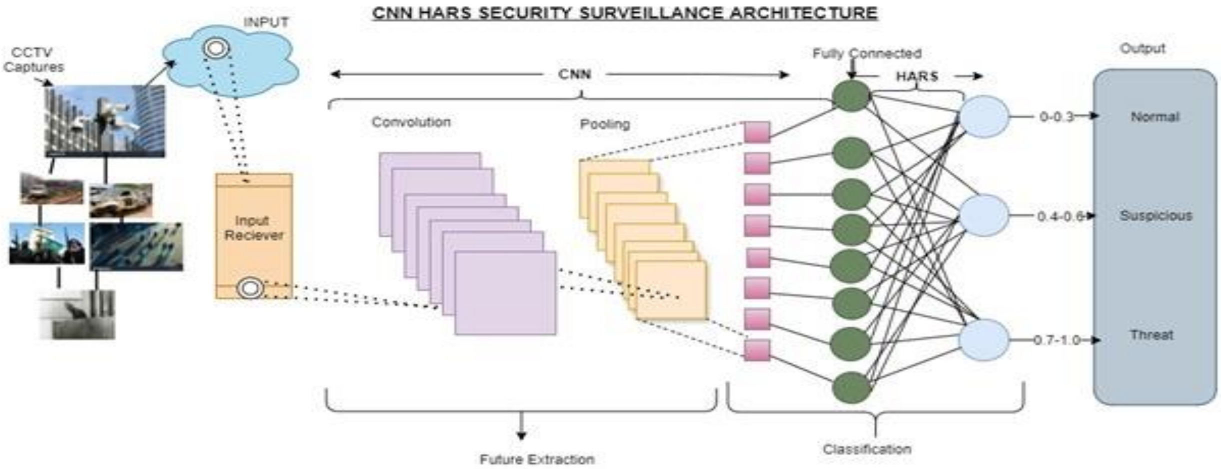
Output and Actions: The final output is categorised into three distinct ranges:
Normal (0.0–0.3): Routine activities like walking or sitting are logged without further action.
Suspicious (0.4–0.6): Activities like loitering or carrying unusual objects trigger alerts to notify security personnel for closer monitoring.

Threat (0.7–1.0): High-risk actions, such as weapon detection or violent behaviour, generate immediate alarms and real-time notifications to security agencies. These include video clips, images, and geolocation data to facilitate rapid intervention.

Continuous Learning and Feedback: The system's accuracy and efficiency rely on continuous training using large, annotated datasets containing diverse images and videos of human activities and objects. Supervised learning techniques enable the model to distinguish between innocuous and threatening behaviours, such as differentiating between a person holding an umbrella and someone holding a weapon.

After deployment, the system undergoes constant refinement through feedback loops from law enforcement agencies and real-time event data. Feedback helps adjust detection thresholds, reducing false positives and improving reliability. The model also incorporates new crime data to adapt to evolving criminal behaviours, ensuring it remains effective over time.

Figure 2
CNN-HARS architecture: showing the integration of convolutional layers, pooling layers, and fully connected layers and human activity recognition for real-time security surveillance.



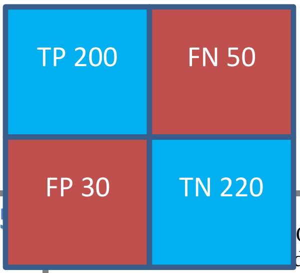
Performance evaluation

To ensure a robust evaluation of the model, the dataset is split into training and test sets at a ratio of 8:2, respectively and utilising the confusion metric to calculate the accuracy, precision, recall and F1-score. The training set is used to train the CNN model, while the test set is reserved for evaluating the model's performance. To handle any class imbalance, **stratified sampling** is employed when splitting the dataset. Stratified sampling ensures that each class, representing different activities, is proportionally represented in both the training and test sets. This is particularly important in HARS applications, where some activities, such as suspicious behaviour, might be less frequent than others, like walking or standing. This ensures that the model gets exposure to all classes, maintaining the distribution of activities as they occur in the real world. The evaluation process involves passing the test data through the trained model and comparing the predicted labels with the actual labels.

Confusion matrix table

Using a test dataset of 500 samples, the performance of the CNN-HARS model is summarised in the confusion matrix presented in **Figure 3**. The model correctly classified 200 true positives and 220 true negatives, while it recorded 30 false positives and 50 false negatives.

Figure3
Confusion matrix table



TP 200	FN 50
FP 30	TN 220

True Positive (TP = 200): These are suspicious activities correctly identified by the model as suspicious.

True Negative (TN = 220): These are normal activities correctly identified by the model as normal.

False Positive (FP = 30): These are normal activities incorrectly flagged by the model as suspicious (false alarm).

False Negative (FN = 50): These are suspicious activities that the model failed to detect, incorrectly classifying them as normal (missed threats).

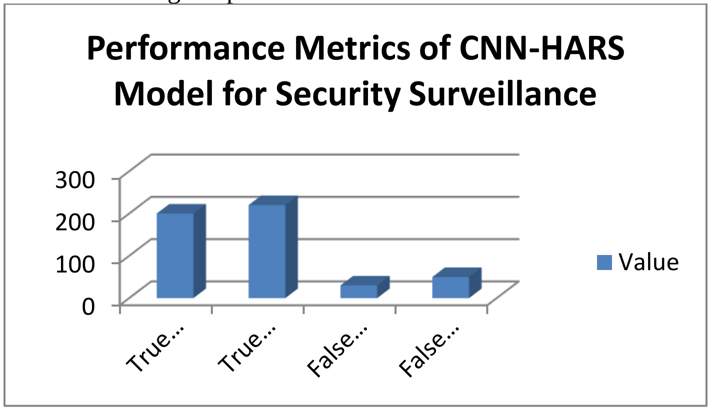
racy $= \frac{\text{TP+TN}}{\text{TP+TN+FP+FN}} = \frac{200+220}{200+220+30+50} = 0.84 = 84\%$

cision $= \frac{\text{TP}}{\text{TP+FN}} = \frac{200}{200+30} = 0.8696 = 86.96\%$

Recall $= \frac{\text{TP}}{\text{TP+FN}} = \frac{200}{200+50} = 0.80 = 80\%$

F1 - Score equalsScore$= 2 * \frac{\text{Precision}* \text{Recall}}{\text{Precision+Recall}} = 2 * \frac{0.8696*0.8}{0.8696+0.8} = 0.833 = 83.3\%$

Figure 4
A chart showing the performance evaluation of the CNN-HARS Model



Discussion
The CNN-HARS model has demonstrated robust performance with high accuracy and balanced precision-recall metrics, especially in detecting suspicious activities crucial for security.

The model achieved an accuracy of 84%, indicating that it correctly predicted the majority of activities in the test data. This high accuracy reflects the system's overall reliability in distinguishing between normal and suspicious activities. The precision score of 86.96% highlights the model's ability to minimize false alarms. This means that most of the activities flagged as suspicious were indeed correct, reducing the likelihood of unnecessary interventions or false alerts in the security system.

However, the recall score of 80% reveals a critical area for improvement. While the model successfully identified a majority of the actual suspicious activities, it failed to detect 20% of such events. In the context of security and threat detection, such omissions may carry serious consequences, making recall a vital metric that must be improved to ensure maximum threat coverage. To address this limitation, several enhancements are proposed for future iterations of the system:

Advanced data augmentation: Applying a broader range of augmentation techniques (e.g., random occlusion, varying lighting conditions, noise injection, temporal jittering) can increase data diversity and reduce over-fitting, making the model more sensitive to underrepresented or subtle threat patterns.

Model hybridisation: Integrating the CNN with temporal models such as Long Short-Term Memory (LSTM) networks or Transformers can improve the system's capacity to recognise sequences of movements and subtle changes in behaviour over time. While CNNs excel at spatial feature extraction, LSTM and Transformer architectures can model temporal dependencies that are often critical in accurately identifying suspicious activity.

Class rebalancing and cost-sensitive learning: Introducing class-weighted loss functions or synthetic oversampling (e.g., SMOTE) for minority threat classes may ensure that the model pays more attention to rare but high-impact suspicious events.

The F1-score of 83.3%**,** which balances precision and recall, confirms the model's strong general performance, but improving recall will make it even more reliable and actionable in real-world scenarios. The CNN-HARS model offers a promising approach to intelligent surveillance in Imo State. To ensure its practical effectiveness, the model needs to be optimised to improve recall, thereby strengthening its ability to reliably detect threats in live security deployments.

Limitations and future work

Despite strong performance, some limitations remain. The system depends heavily on clear visual input, which may reduce accuracy in poor weather or low-visibility conditions. It also requires significant computational resources for real-time analysis, which could hinder large-scale deployment. Future efforts should aim to improve performance in low-visibility scenarios and reduce resource demands to enable broader use across multiple surveillance zones.

Conclusion

In conclusion, while security agencies in Imo State have made efforts to combat crime, the current surveillance methods are plagued by numerous shortcomings. These shortcomings, including inadequate technological tools, poor coordination among security agencies, and the rapid evolution of criminal tactics, have hindered effective crime prevention and response. As criminal activities continue to evolve, there is an urgent need to enhance the state's surveillance capabilities with more advanced technologies and a more integrated approach to policing. Only through the adoption of smarter, technology-driven solutions, such as AI-based surveillance systems, drones, and enhanced inter-agency collaboration, will Imo State be able to address its growing insecurity effectively. The introduction of these technologies could improve intelligence gathering, monitoring, and response times, ultimately making the state a safer place for its residents.

Reference

Abimbola, A. (2024**).** *Anxiety, fear of public buses… How a one-chance robbery affects commuters' mental health*. Foundation for Investigative Journalism. https://fij.ng/article/anxiety-fear-of-public-buses-how-one-chance-robbery-affects-commuters-mental-health/

Achumba, I. C., Ighomereho, O. S., & Akpan-Robaro, M. O. M. (2013). Security challenges in Nigeria and the implications for business activities and sustainable development. *Journal of Economics and Sustainable Development, 4*(2), 79–99.

Adeleke, A. S., Angela, M., & Oliver, S. (2022). *Organized crime in Nigeria: A threat assessment*. United Nations Office on Drugs and Crime (UNODC) and National Institute for Security Studies (NISS).

Ali, S., Rahman, M., & Zhang, H. (2020). Real-time human activity recognition for enhanced surveillance systems using deep learning. *International Journal of Advanced Computer Science and Applications, 11*(5), 56–65.

Cheng, L., Wang, Y., & Liu, Z. (2019). Challenges and advancements in human activity recognition under real-world conditions. *Computer Vision and Pattern Recognition Journal, 8*(4), 421–435.

Cite this article as:
Ohanaka, B. U., Michael, O. D., Udeogu C., Bardi, I. A., & Odoemene,I. O. (2025). Leveraging a hybridized CNN-HARS surveillance model for security threat detection in Imo State, Nigeria. *FNAS Journal of Computing and Applications, 2*(3), 52-61. https://doi.org/10.63561/jca.v2i3.836

Chigozie, U. (2020). Imo State security network: Bridging the gap in local and federal crime prevention strategies. *African Journal of Security Studies, 15*(2), 112–124.

Glorot, X., Bordes, A., & Bengio, Y. (2011). Deep sparse rectifier neural networks. In *Proceedings of the 14th International Conference on Artificial Intelligence and Statistics* (Vol. 15, pp. 315–323).

Goodfellow, I., Bengio, Y., & Courville, A. (2016). *Deep learning*. MIT Press.

Kim, S., Park, Y., & Kim, J. (2019). Drone-based human activity recognition using deep learning for surveillance applications. *Journal of Intelligent & Robotic Systems*, *96*(3–4), 401–414.

Kingma, D. P., & Ba, J. (2015). Adam: A method for stochastic optimization. In *Proceedings of the International Conference on Learning Representations (ICLR)*.

Krizhevsky, A., Sutskever, I., & Hinton, G. E. (2012). ImageNet classification with deep convolutional neural networks. *Advances in Neural Information Processing Systems*, *25*, 1097–1105.

Lara, O. D., & Labrador, M. A. (2013). A survey on human activity recognition using wearable sensors. *IEEE Communications Surveys & Tutorials, 15*(3), 1192–1209.

LeCun, Y., Bottou, L., Bengio, Y., & Haffner, P. (1998). Gradient-based learning applied to document recognition. *Proceedings of the IEEE, 86*(11), 2278–2324.

Liu, W., Anguelov, D., Erhan, D., Szegedy, C., Reed, S., Fu, C. Y., & Berg, A. C. (2016). SSD: Single Shot MultiBox Detector. In *European Conference on Computer Vision* (pp. 21–37). Springer

Niemann, T., Hoffmann, L., & Zhang, Y. (2018). Advances in deep learning for human activity recognition. *Machine Learning Applications in Security, 19*(2), 98–109.

Nwachukwu, I., Ugochukwu, M., & Ogbonna, E. (2022). The socio-economic impact of violent crimes in Imo State. *Journal of African Studies, 13*(4), 102–118.

Nwankwo, K., & Okafor, S. (2023). Armed robbery and its implications for security in Imo State: A policy perspective. *Journal of Criminology and Public Policy, 28*(3), 209–221.

Okafor, J., & Udo, C. (2021). Political tensions and security challenges in southeastern Nigeria. *Africa Political Review, 9*(3), 150–166.

Oketa, C. M. (2018). Socio-economic implication of kidnapping and hostage taking in southern Nigeria. *South-East Journal of Public Relations*, *1*(1).

Omenga, J. (2013). Section 14(2) of the 1999 Constitution of the FRN in the light of reason. *NAJOPS, 9*(2). Retrieved March 13, 2024, from

Opara, I., Nkem, E., & Adiele, U. (2022). Artificial intelligence in crime prevention: Applications and challenges. *International Journal of Security Technology, 17*(1), 56–71.

Otuu, O., Nwabuaku, W. K., & Ugwu, C. C. (2022). Efficacy of community policing and its funding for public security: A study of Imo vigilante groups in Imo State. *International Journal of Scientific & Engineering Research, 13*(6), 244.

Redmon, J., Divvala, S., Girshick, R., & Farhadi, A. (2016). You Only Look Once: Unified, real-time object detection. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 779–788).

Ren, S., He, K., Girshick, R., & Sun, J. (2015). Faster R-CNN: Towards real-time object detection with region proposal networks. In *Advances in Neural Information Processing Systems, 28*, 91–99.

Srivastava, N., Hinton, G., Krizhevsky, A., Sutskever, I., & Salakhutdinov, R. (2014). Dropout: A simple way to prevent neural networks from overfitting. *Journal of Machine Learning Research*, *15*, 1929–1958.

Wang, J., Chen, Y., Hao, S., Peng, X., & Hu, L. (2018). Deep learning for sensor-based activity recognition: A survey. *Pattern Recognition Letters*, *119*, 3–11.

Zhang, Q., Li, W., & Yang, X. (2021). The role of deep learning in advancing human activity recognition systems. *Journal of Applied Artificial Intelligence*, *15*(6), 67–83.

Zhu, X., Zhou, L., & Han, J. (2020). Facial recognition integration in surveillance systems: Enhancing security through AI. *Journal of Computer Vision and Applications, 18*(4), 321–340.

Cite this article as:
Ohanaka, B. U., Michael, O. D., Udeogu C., Bardi, I. A., & Odoemene,I. O. (2025). Leveraging a hybridized CNN-HARS surveillance model for security threat detection in Imo State, Nigeria. *FNAS Journal of Computing and Applications, 2*(3), 52-61. https://doi.org/10.63561/jca.v2i3.836