ACTA SCIENTIAE

ISSN: 2178-7727

Detecting Crime Anomalies in Smart Cities with Sharkprey Optimization and Ensemble Machine Learning

Ayush Singhal[1] and Niraj Singhal[2], Pradeep Kumar[3]

[1]Research Scholar, Department of Computer Science & Engineering, Shobhit Institute of Engineering & Technology, (NAAC Accredited Grade "A", Deemed to- be-University), Meerut (250110), India
Assistant Professor, Department of Computer Science and Engineering, Meerut Institute of Technology, Meerut
[2]Director, Sir Chotu Ram Institute of Engineering & Technology, C.C.S. University, Meerut, India
[3]Assistant Professor, JSS Academy of Technical Education, Noida, Uttar Pradesh, India

ABSTRACT

The advent of smart cities has enabled the creation of automated criminal anomaly detection systems, owing to the copious urban data streams. This study explores the use of machine learning techniques to evaluate and identify abnormal patterns in criminal incidents. This technology improves proactive law enforcement methods, streamlines resource allocation, and helps create safer and more secure urban environments by using real-time data from several sources.In the first stage, video data is gathered from a network of strategically placed surveillance cameras across the intelligent urban area. The automated criminal anomaly detection system may be trained and improved by using this comprehensive video collection, enabling it to accurately identify and distinguish between normal and abnormal behavior patterns in varied urban settings. The collected data is subjected to preprocessing utilizing Video-to-Frame Conversion, Non-Local Means (NLM), and contrast stretching approach. The Sobel edge detection technique is used to discover the Regions of Interest (ROI) inside the frames for the purpose of segmentation, using the pre-processed data. This method integrates the White Shark Optimizer with Osprey optimization technique. Create an innovative ensemble machine learning approach to identify criminal abnormalities by combining the K-Nearest Neighbors, Random Forest, and optimum Artificial Neural Network models. To improve the precision of detection, the weight of the Artificial Neural Network (ANN) is fine-tuned using the Sharkprey Optimization approach. MATLAB is used for the execution.

KEYWORDS: Gradient Interpolation-Based Hog Model, Improved Gradient Local Binary Patterns,Smart cities,Crime detection,Sharkprey Optimization Algorithm

INTRODUCTION

The increase in crime rates is the primary cause of loss of life and property in the twenty-first century, when compared to other issues. An intelligent video surveillance system is the preferred choice for promptly and accurately identifying unusual situations. The wide-ranging uses of abnormal event detection in surveillance recordings, such as deterring crime, automating intelligent visual surveillance, and ensuring traffic security, need significant attention [1,2]. In recent decades, a significant number of security cameras have been implemented in both public and private areas to provide prompt and continuous surveillance, with the aim of averting mishaps and guaranteeing public well-being [3].

Surveillance of regions with a high probability of criminal activity has grown difficult as a result of the recent surge in urban population. The absence of authority in these regions has led to a surge in crime and instability. The emergence of smart city infrastructure offers an opportunity to provide innovative solutions to these problems [4].A "smart city" is a metropolitan region that is equipped with advanced technology and integrated systems to allow efficient and sustainable management[5]. This essential infrastructure improves the quality of life for its residents by offering city navigation, public safety, social welfare services, transportation, real estate, healthcare, and tourist services[6].A "smart city" is mostly propelled by information and communication technologies (ICTs) [7,8].

DOI: https://doi.org/10.57030/ASCI.25.4.AS24

ISSN: 2178-7727

An "anomaly" refers to unforeseen occurrences or crises that deviate from the norm, expectations, or established standards. Irregularity detection plays a crucial role in managing smart cities, such as traffic control and illegal exploration [9]. Traditionally, experts have had to engage in constant video monitoring in order to identify unexpected happenings. It consistently becomes a challenging and laborious undertaking. Research efforts related to developing a practical detection technique are very important because they may reduce the number of personnel required to monitor videos, particularly in surveillance systems [10].The core focus of any ecosystem designed for a smart city is on ensuring robust security measures and safeguarding privacy. It is essential to protect the security of every entity at all times. A novel security mechanism is being devised to address the varied security needs of a typical smart city. This is necessary because traditional security techniques are inadequate in addressing all the different aspects and scenarios of a smart city due to various limitations such as scalability, heterogeneity, power, storage, and computational capabilities [11].Anomaly detection may reduce the risk of crime or other undesired actions, hence enhancing security. ML algorithms are among the several techniques developed for detecting anomalies [13]. To establish an effective anomaly detection system, it is necessary to further improve the performance of these approaches. Therefore, a new hybrid optimization approach was created.

The study is structured methodically into significant parts, each of which enhances the understanding and evaluation of the proposed automated criminal anomaly detection system. The second portion provides a comprehensive examination of prior research and completed projects in the topic. The mechanism for detecting criminal anomalies is comprehensively explained in Section 3 to provide readers with a deep comprehension of the system's architecture.A detailed analysis of the results achieved using the suggested model is presented in section 4. The conclusion may be found in the fifth part.

REVIEW OF EXISTING LITERATURE

In 2021, Cauteruccio et al.[14] made an early attempt to investigate abnormalities in a MIoT. To streamline the process, a novel methodological framework is proposed. Firstly, let's define the terms "forward problem" and "inverse problem" in the context of anomaly detection in a MIoT (Machine-to-Internet of Things) system. The description of these concerns allows for the examination of the connections between anomalies and the distances between nodes, the size of the IoT network, the centrality of nodes in terms of their degree, and the centrality of nodes in terms of their proximity. The solution proposed in this case was implemented in a smart city setting, which is a common example of a MIoT (Mobile Internet of Things) scenario.

In 2022, Girdhar et al.[15] introduced a framework for CAV-enabled mobility that is very flexible and capable of accommodating any cyber-based organizations. Moreover, the effectiveness of an autonomous system relies on its capacity to make accurate determinations in real-time. However, cyber assaults on these objectives might hinder this capacity, leading to intricate mishaps involving connected and autonomous vehicles (CAVs). Additionally, proposed a 5Ws and 1H-based investigative method to address cyberattack-related accidents, since the existing accident investigation frameworks were inadequate in understanding and handling such incidents.

In their 2017 publication, Khatoun et al.[16] elucidated the fundamental concepts behind the design of smart cities, while also providing an assessment of ongoing efforts and projects. Next, we examined a range of privacy and security problems, suggestions, and benchmarks for smart cities and their services. Subsequently, we identified and resolved many security vulnerabilities and privacy issues associated with smart cities.

In 2021, Ashraf et al. introduced a novel system, namely IoTBoT-IDS, for safeguarding IoT-based smart networks against botnet assaults. The IoTBoT-IDS utilizes BMM and Correntropy models, which are statistical learning approaches, to effectively capture the usual behavior of IoT networks. Any deviation from the standard was acknowledged as an abnormal occurrence. IoTBoT-IDS was evaluated using three benchmark datasets generated by real IoT networks.

In 2022, Shin et al.[18] presented a security service's anomaly detection system that relies on a surveillance

DOI: https://doi.org/10.57030/ASCI.25.4.AS24

ISSN: 2178-7727

map. A two-stage anomaly detection system was developed specifically for exceptional situations. This facilitated the identification of atypical situations, such as abnormal gatherings of individuals, vehicular motion, unfamiliar items, and changes in temperature. The suggested data architecture has the potential to be used in many applications within the smart city context. This is due to the surveillance map, which facilitates efficient and cohesive analysis of extensive multimodal data from several agents.

In 2020, Rashid et al.[19] conducted a study on a machine learning-based method for detecting and countering cybersecurity risks in the Internet of Things (IoT) in a smart city. Subsequently, an examination was conducted on ensemble approaches such as bagging, boosting, and stacking in order to enhance the efficiency of the detection system. This is in contrast to previous studies that focused just on individual classifiers. The current discussion focuses on the incorporation of feature selection, cross-validation, and multi-class classification in the given domain. This particular topic has not been extensively explored in existing literature.

In 2021, Ma et al.[20] conducted a comprehensive analysis of the existing literature on security in that particular technology. They also provided explanations on cyber security, smart cities, and other related subjects. To accomplish this, the study focused on the four essential components of a smart city: intelligent power grid, intelligent infrastructure, intelligent transportation, and intelligent healthcare. The presentation included a concise overview of two deep learning techniques, efforts in the field of cyber-security, and the correlation between technology and smart cities. Furthermore, the discussion included effective strategies for preserving user privacy and ensuring cyber security in smart cities.

In 2018, Garcia-Font et al.[21] assessed Support Vector Machines (SVM) and Random Forests as two Machine Learning (ML) algorithms for detecting anomalies in a laboratory setting that replicated a real-life scenario for a smart city, including diverse devices and network configurations. The experience has enabled us to showcase that, notwithstanding the significance of these strategies for smart cities, supplementary aspects must be considered to precisely identify assaults. Table 1 displays the research gaps identified in the reviews conducted by different authors.

METHODOLOGY PROPOSAL

Machine learning and computer vision technologies are crucial for detecting unusual criminal activities in smart cities. Smart city infrastructure incorporates surveillance cameras strategically positioned across the city to monitor criminal activities and uphold public safety. Nevertheless, the manual surveillance of these cameras is both laborious and inefficient. Given this information, there is a strong need for automated systems that can detect and identify illicit activities. Crime detection systems that identify abnormal behavior, theft, and violence use several methodologies. Usually, these systems operate in the way shown in Figure 1.

DOI: https://doi.org/10.57030/ASCI.25.4.AS24

ISSN: 2178-7727

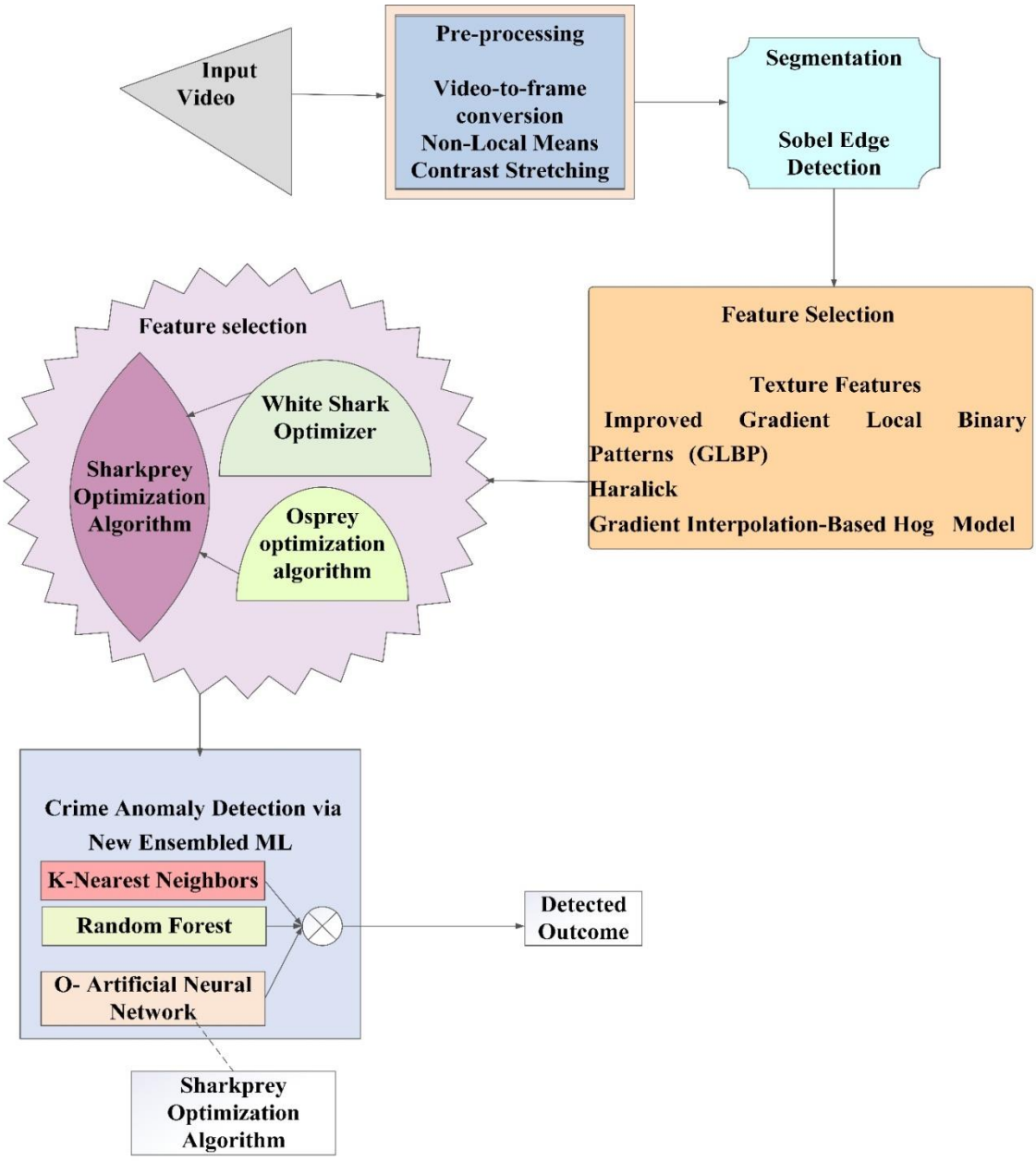

Figure 1: Proposed Flow

RESULT AND DISCUSSION

Metrics for measuring performance

- FNR: commonly referred to as the "miss rate," quantifies the probability of a test failing to detect a genuine positive.
- FPR: The false positive rate is calculated by dividing the total number of incorrect classifications of adverse facts as unfavourable by the number of adverse facts.
- NPV: NPV is a statistical metric that evaluates the reliability of a negative test result in a group of individuals with a certain disease. The deliberate action involves dividing the overall population that is unaffected by the situation by the specific number of adverse consequences.
- MCC: The MCC metric is used to evaluate the performance of binary classification models. The Matthews Correlation Coefficient (MCC) is a reliable statistic for assessing the performance of binary classifiers since it considers true positives (TP), true negatives (TN), false negatives (FN), and false positives (FP).
- F-Measure: This metric achieves a balance by ensuring that each definition expressly refers to just one sort of information item and completely determines each data bit.

DOI: https://doi.org/10.57030/ASCI.25.4.AS24

ISSN: 2178-7727

- Accuracy: The accuracy metric, which measures the ratio of correct predictions to total predictions, is a simple and often used classification statistic.

The UCF-Crime dataset comprises 128 hours of films and is notably comprehensive. The collection consists of 1900 unedited, extensive reality surveillance recordings, which include 13 authentic irregularities such as mistreatment, arson, assault, road accidents, robberies, eruptions, fights, theft, gunshots, robbery, and vandalism. The anomalies were chosen because they have a significant impact on public safety.This dataset may be used to do two objectives effectively. Initially, a comprehensive examination of anomalies is conducted, considering all anomalies as a collective and all routine operations as a separate entity. Furthermore, to accurately identify each of the 13 peculiar behaviors.

The recommended model is implemented using the MATLAB programming language. This section provides a detailed explanation of the graphical analysis used in the Automated Crime Anomaly Detection system for Smart Cities. This section discusses the execution metrics used to evaluate the performance of the proposed model and compares it with previous methodologies.

Table 1: Proposed Vs Exiting

Methods	MCC	FNR	FPR	NPV	F-Measure	Precision	Acc	Spec	Sen
Proposed	0.894	0.097	0.007	0.9923	0.902	0.902	0.986	0.992	0.902
ANN	0.843	0.145	0.011	0.988	0.854	0.854	0.979	0.988	0.854
KNN	0.805	0.180	0.013	0.986	0.819	0.819	0.974	0.986	0.819
Random Forest	0.821	0.165	0.012	0.987	0.834	0.834	0.976	0.987	0.834
Decision Tree	0.595	0.375	0.028	0.971	0.624	0.624	0.946	0.971	0.624
AdaBoost	0.674	0.302	0.023	0.976	0.697	0.697	0.956	0.976	0.697

The KNN approach demonstrates its accuracy in categorizing positive and negative cases with a specificity of 0.986 and a sensitivity of 0.819, respectively. It demonstrates a high level of proficiency in making precise predictions, with a 0.974 accuracy rate. The positive predictions of the system are very accurate, as shown by its precision score of 0.819. Additionally, the F-measure of 0.819 demonstrates a well-balanced compromise between precision and sensitivity. The method's NPV of 0.986 indicates its strong ability to accurately forecast unfavorable events. Additionally, it maintains a low False Negative Rate (FNR) of 0.180 and a False Positive Rate (FPR) of 0.013, indicating its commitment to minimizing mistakes in both kinds of classifications. The MCC score of 0.805 indicates the overall predictability of the data.Random Forest has the best success percentage in accurately recognizing positive events, with a sensitivity score of 0.834. It demonstrates exceptional accuracy in accurately categorizing negative cases, with a specificity of 0.987. The approach continues to provide precise predictions overall, as seen by its accuracy score of 0.976. The F-measure of 0.834 demonstrates a well-balanced performance in terms of precision and sensitivity, while its precision score of 0.834 highlights its accuracy in making optimistic predictions. The significant NPV of 0.987 displays its ability to precisely predict unfavorable scenarios. The method's effectiveness in minimizing classification mistakes is supported by its low false positive rate (FPR) of 0.012 and false negative rate (FNR) of 0.165. The MCC score of 0.821 demonstrates the overall predictability of the outcome.

The decision tree has a sensitivity of 0.624. It showcases its capacity to accurately categorize negative cases with a specificity of 0.971. The total accuracy, indicating the capacity to generate precise predictions for both classes, is 0.946. The precision score of 0.624 suggests that its positive prediction accuracy is somewhat lower. The F-measure of 0.624 demonstrates an equitable compromise between sensitivity and accuracy. The approach has high efficacy in accurately forecasting negative situations, as shown by its Negative Predictive Value (NPV) of 0.971. It reduces the number of real negatives that are mistakenly classified as positives, while

DOI: https://doi.org/10.57030/ASCI.25.4.AS24

ISSN: 2178-7727

keeping the false positive rate (FPR) reasonably low at 0.028. Although the false negative rate (FNR) of 0.375 is quite high, it indicates that the system is more effective at detecting false positives than real positives.

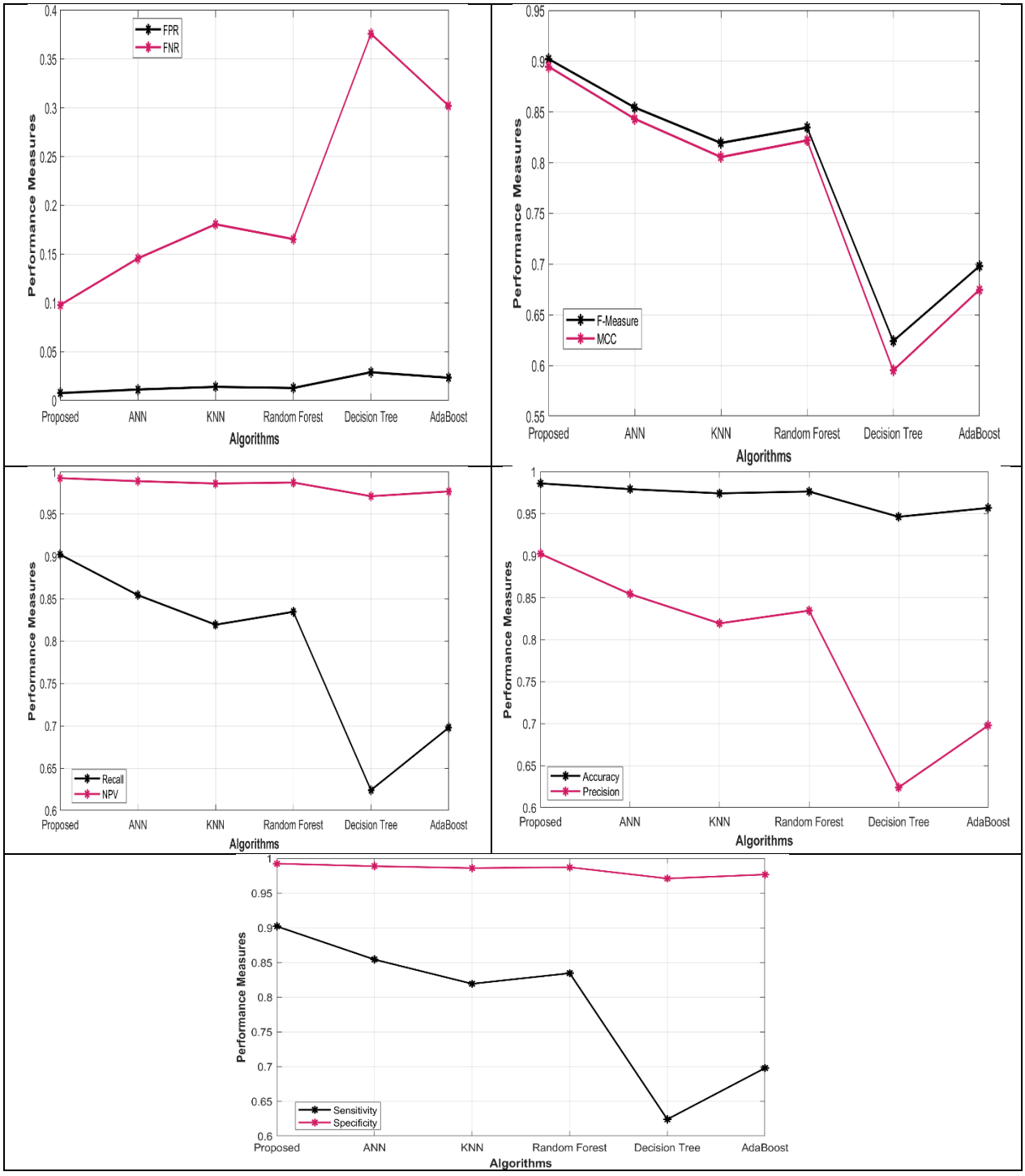

Figure 2: Graphical Representation of Performance Metrics

The MCC score of 0.595, which represents the total prediction quality, concludes.TheAdaBoost approach has a sensitivity of 0.697, indicating its high accuracy in detecting positive cases. It shows its proficiency in properly categorizing negative events with a specificity of 0.976. The system's total accuracy, which quantifies its capacity to provide precise predictions for both classes, is 0.956. The precision score of 0.697 highlights the accuracy of its optimistic forecasts. The F-measure of 0.697 highlights the well-balanced trade-off between accuracy and sensitivity. The method's NPV of 0.976 indicates its strong ability to accurately anticipate negative situations. The FPR of 0.023 indicates that it effectively reduces the misclassification of real negatives as positives. With a false negative rate (FNR) of 0.302, it indicates a lower number of correctly

DOI: https://doi.org/10.57030/ASCI.25.4.AS24

ISSN: 2178-7727

identified positive cases. The MCC score of 0.674 indicates the overall accuracy of the forecasts. Figure 2 depicts the visual depiction of the Performance results.

CONCLUSION

The integration of the Sharkprey Optimisation Algorithm with an Ensembled-Machine Learning Approach offers a robust approach for detecting criminal anomalies in smart cities. By using this state-of-the-art combination, the process of identifying anomalies became more precise and effective. Additionally, the system demonstrated its adaptability in various metropolitan settings.Prior to any analysis, it is necessary to get video data from the extensive network of security cameras installed across the smart city. The criminal anomaly detection system may be trained and improved using this large video collection to identify normal and aberrant behavior patterns in various urban environments. The acquired data is preprocessed using the Video-to-Frame Conversion, NLM, and contrast stretching techniques. The Sobel edge detection technique was used to determine the region of interest (ROI) in the frames for segmentation from the pre-processed data. Extracted features from the segmented areas using I-GLBP, Haralick, and GI-HOG.Utilizing the Sharkprey Optimization Algorithm, which combines the WSO and Osprey optimization algorithms, modify the retrieved characteristics to eliminate any superfluous or duplicate features. Developed a novel ensemble machine learning approach for identifying unusual criminal activities based on selected characteristics by combining the K-Nearest Neighbors (KNN), Random Forest (RF), and Optimal Artificial Neural Network (O-ANN) algorithms. The weight of the artificial neural network (ANN) was calibrated using the novel hybrid optimization approach to enhance the accuracy of detection. The implementation use MATLAB.

REFERENCE

[1]. Ullah, W., Ullah, A., Hussain, T., Khan, Z.A. and Baik, S.W., 2021. An efficient anomaly recognition framework using an attention residual LSTM in surveillance videos.Sensors, 21(8), p.2811.

[2]. Xu, X., Liu, L., Zhang, L., Li, P. and Chen, J., 2020. Abnormal visual event detection based on multi-instance learning and autoregressive integrated moving average model in edge-based Smart City surveillance. Software: Practice and Experience, 50(5), pp.476-488.

[3]. Shao, Z., Cai, J. and Wang, Z., 2017. Smart monitoring cameras driven intelligent processing to big surveillance video data. IEEE Transactions on Big Data, pp.105-116.

[4]. Kitchin, R. and Dodge, M., 2020. The (in) security of smart cities: Vulnerabilities, risks, mitigation, and prevention. In Smart Cities and Innovative Urban Technologies (pp. 47-65). Routledge.

[5]. Saravanan, K., Julie, E.G. and Robinson, Y.H., 2019. Smart cities & IoT: Evolution of applications, architectures & technologies, present scenarios & future dream. Internet of things and big data analytics for smart generation, pp.135-151.

[6]. Hassan, S.U., Shabbir, M., Iqbal, S., Said, A., Kamiran, F., Nawaz, R. and Saif, U., 2021. Leveraging deep learning and SNA approaches for smart city policing in the developing world. International Journal of Information Management, 56, p.102045.

[7]. Attaran, H., Kheibari, N. and Bahrepour, D., 2022. Toward integrated smart city: A new model for implementation and design challenges. GeoJournal, 87(Suppl 4), pp.511-526.

[8]. Balfaqih, M. and Alharbi, S.A., 2022. Associated Information and Communication Technologies Challenges of Smart City Development.Sustainability, 14(23), p.16240.

[9]. Chen, N. and Chen, Y., 2022. Anomalous vehicle recognition in smart urban traffic monitoring as an edge service.Future Internet, 14(2), p.54.

[10]. Zhao, Y., Man, K.L., Smith, J. and Guan, S.U., 2022. A novel two-stream structure for video anomaly detection in smart city management.The Journal of Supercomputing, 78(3), pp.3940-3954.

[11]. Ahad, M.A., Paiva, S., Tripathi, G. and Feroz, N., 2020. Enabling technologies and sustainable smart cities.Sustainable cities and society, 61, p.102301.

[12]. Kumar, P., Kumar, R., Srivastava, G., Gupta, G.P., Tripathi, R., Gadekallu, T.R. and Xiong, N.N., 2021. PPSF: A privacy-preserving and secure framework using blockchain-based machine-learning for IoT-driven smart cities. IEEE Transactions on Network Science and Engineering, 8(3), pp.2326-2341.

[13]. Islam, M., Dukyil, A.S., Alyahya, S. and Habib, S., 2023. An IoT Enable Anomaly Detection System for Smart City Surveillance.Sensors, 23(4), p.2358.

DOI: https://doi.org/10.57030/ASCI.25.4.AS24

ISSN: 2178-7727

[14].Cauteruccio, F., Cinelli, L., Corradini, E., Terracina, G., Ursino, D., Virgili, L., Savaglio, C., Liotta, A. and Fortino, G., 2021. A framework for anomaly detection and classification in Multiple IoT scenarios.Future Generation Computer Systems, 114, pp.322-335.

[15].Girdhar, M., You, Y., Song, T.J., Ghosh, S. and Hong, J., 2022. Post-accident cyberattack event analysis for connected and automated vehicles.IEEE Access, 10, pp.83176-83194.

[16].Khatoun, R. and Zeadally, S., 2017. Cybersecurity and privacy solutions in smart cities.IEEE Communications Magazine, 55(3), pp.51-59.

[17]. Ashraf, J., Keshk, M., Moustafa, N., Abdel-Basset, M., Khurshid, H., Bakhshi, A.D. and Mostafa, R.R., 2021. IoTBoT-IDS: A novel statistical learning-enabled botnet detection framework for protecting networks of smart cities. Sustainable Cities & Soc., p.103041.

[18]. Shin, H., Na, K.I., Chang, J. and Uhm, T., 2022. Multimodal layer surveillance map based on anomaly detection using multi-agents for smart city security. ETRI Journal, 44(2), pp.183-193.

[19]. Rashid, M.M., Kamruzzaman, J., Hassan, M.M., Imam, T. and Gordon, S., 2020. Cyberattacks detection in iot-based smart city applications using machine learning techniques.Int. Journal of environmental research and public health, 17(24), p.9347.

[20]. Ma, C., 2021. Smart city and cyber-security; technologies used, leading challenges and future recommendations. Energy Reports, 7, pp.7999-8012.

[21]. Garcia-Font, V., Garrigues, C. and Rifà-Pous, H., 2018. Difficulties and challenges of anomaly detection in smart cities: A laboratory analysis. Sensors, 18(10), p.3198.

DOI: https://doi.org/10.57030/ASCI.25.4.AS24