International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 03 | March - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

Anomaly Detection Using CNN with I3D Feature Extraction

A.Nandini[1] , Ashifa.K[1] , B.Jyoshnapriya[1]
K.R.Jayavelu[2],J.Jayaprakash[2],G.Victo Sudha George[2]
[1] IVYear B.Tech, Dept of CSE,[2] Professor,Dept of CSE
[1]nandininaidu450@gmail.com,[1]ashifabasheer19@gmail.com,[1]jyoshnapriya250101@gmail.com
[1,2] DR. M.G.R EDUCATIONAL AND RESEARCH INSTITUTE,Maduravoyal, Chennai-95, Tamil Nadu,India

Abstract— Anomaly detection is a critical task in various fields such as surveillance, healthcare, and industrial monitoring, aiming to identify patterns that deviate significantly from normal behavior.Video anomaly detection is inherently difficult due to visual complexity and variability. This work proposes a unique anomaly detection technique leveraging Convolutional Neural Networks (CNN) with Inflated 3D Convolutional Networks (I3D) for feature extraction. This involves training the CNN on a large dataset to learn normal behavior, enabling it to identify anomalies by recognizing deviations from learned patterns. Furthermore, our approach exhibits promising results in detecting various types of anomalies, including sudden changes, abnormal trajectories, and rare events. Upon detection of such activity, mail(notification) can be raised concerned people who can take immediate action.This research contributes a significant advancement in the field of anomaly detection, and holds potential for applications in surveillance, security, and industrialmonitoring systems.

Keywords—*Anomaly detection,I3D(Inflated3D) feature extraction,Convolutional neural network, Spatio-Temporal Features,Normal and abnormal event detection.*

1. INTRODUCTION

Anomaly detection, a pivotal task in various domains including surveillance, healthcare, and finance, employs advanced techniques to identify deviations from normal patterns or behaviors. Leveraging Convolutional Neural Networks (CNNs) and Inflated 3D Convolutional Networks (I3D) for feature extraction has emerged as a potent approach due to their efficacy in capturing spatial and temporal information from data. CNNs, originally developed for image processing tasks, excel at learning hierarchical representations of video data. Leveraging convolutional layers, pooling, and non-linear activations, CNNs can extract key features from images, removing noise and creating clearer representations, extract discriminative features from images, enabling them to discern intricate patterns and structures.I3D, an extension of CNNs designed for video analysis, incorporates 3D convolutions to capture temporal dynamics in addition to spatial information. This architecture enhances the model's capacity to comprehend motion and action sequences, making it particularly suitable for anomaly detection in video data where temporal context is crucial. The integration of CNNs and I3D for feature extraction in anomaly detection involves employing pre-trained models to extract high-level representations from input data. These representations encode meaningful information about normal patterns and behaviors, facilitating the detection of anomalies based on deviations from established norms. In anomaly detection using CNN and I3D feature extraction, this method typically involves the following steps: Data Preprocessing: Prepare the input data, which could be images or video sequences, by resizing, normalizing, and augmenting as necessary to enhance model robustness and generalization. Feature Extraction: Utilize pre-trained CNN and I3D models to extract features from the input data. The CNN extracts spatial features from individual frames, while the I3D captures both spatial and temporal features from video sequences. Feature Fusion: Integrate the extracted features from both CNN and I3D models to create a comprehensive representation of the input data, combining spatial and temporal information effectively. Anomaly Detection: Employ appropriate anomaly detection algorithms, such as clustering, classification, or reconstruction-based techniques, on the fused feature representations to identify deviations from normal patterns. Evaluation and Refinement: Assess the performance of the anomaly detection system using metrics like precision, recall, and F1-score. Refine the model and parameters iteratively to improve detection accuracy and reduce false positives.By leveraging the complementary strengths of CNNs and I3D for feature extraction, anomaly detection systems can achieve enhanced accuracy and robustness in identifying abnormalities in various types of data, thereby contributing to improved decision-making and risk mitigation in diverse applications.

2.LITERATURE REVIEW:

The compilation of academic papers encompasses a wide spectrum of topics related to surveillance, anomaly detection, and crime prediction through various machine learning methodologies. Ranging from innovative applications of image processing in "Traffic surveillance and anomaly detection" to the integration of artificial bee colony algorithms with neural networks for "Hybrid artificial neural network with artificial bee colony algorithm for crime classification," these papers offer diverse insights into cutting-edge techniques. Real-time crime intelligence is addressed through "Enabling Real Time Crime Intelligence Using Mobile GIS and Prediction Methods," while "Unsupervised Spatio-Temporal Embeddings for User and Location Modelling" explores spatial and temporal modeling. Technological advancements like convolutional neural networks are leveraged in "Crime scene prediction by detecting threatening objects," and the role of ensemble approaches is discussed in "Survey paper on crime prediction using ensemble approach." Overall, the collection reflects the interdisciplinary nature of crime prediction research, showcasing advancements in machine learning, data mining, and spatial-temporal modeling for comprehensive analysis and forecasting.

International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 08 Issue: 03 | March - 2024 SJIF Rating: 8.176 ISSN: 2582-3930

Leveraging innovative techniques in anomaly detection and crime prediction several noteworthy contributions have been made. The paper titled "Anomaly detection in crowds using multi-sensory information" explores the utilization of multi- sensory data for detecting anomalies in crowded environments. Another significant work, "GeST: A grid embedding based spatio-temporal correlation model for crime prediction," introduces a novel grid embedding approach for spatio-temporal correlation modeling in crime prediction scenarios. Additionally, "Hyperspectral Anomaly Detection via Background and Potential Anomaly Dictionaries Construction" addresses hyperspectral anomaly detection through the construction of background and potential anomaly dictionaries. These studies collectively showcase the diverse methodologies and technologies applied in advancing anomaly detection and crime prediction research, underscoring the interdisciplinary nature of this field.

The paper titled "Anomaly Detection of Railway Catenary Based on Deep Convolutional Generative Adversarial Networks" presents a significant contribution to anomaly detection in the railway domain. Focusing on the catenary system, the study employs Deep Convolutional Generative Adversarial Networks (DCGANs) as a robust methodology. By leveraging the power of generative adversarial networks in learning intricate patterns and representations, the proposed model demonstrates effectiveness in identifying anomalies within the railway catenary system. The utilization of deep convolutional architectures enhances the network's ability to discern subtle variations and abnormalities, thereby providing a promising approach for ensuring the reliability and safety of railway infrastructures. This research exemplifies the application of cutting-edge deep learning techniques for anomaly detection in critical transportation systems, contributing to advancements in railway infrastructure monitoring and maintenance.

3.PROBLEM STATEMENT:

Anomalous events take place rarely as compared to normal activities.Despite widespread deployment of surveillance cameras in cities, effectively monitoring for infrequent yet critical crime activities like chain snatching, attempted murder, or other rare events remains a daunting task. Human analysts simply cannot keep up with the sheer volume of footage, nor can they consistently maintain the focus and attention required to detect these subtle or fleeting actions.

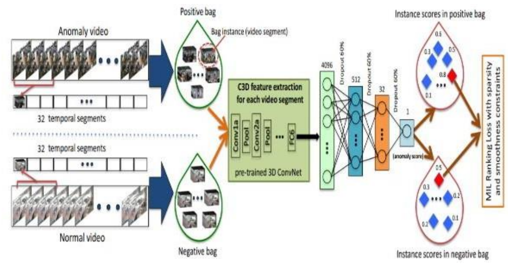
If it is normal situation there's nothing problem if it is abnormal then the problem is raised.

Data quality issues and small training samples makes anomaly detection algorithm complicated.

4.EXISTING SYSTEM:

In the first phase, the object was detected using background subtraction and from frame sequences the object is extracted. The second phase was detection of suspicious activity. Advantage of the system was the algorithm works on real time video processing and its computational complexity was low. Storage limitations hampered the system's effectiveness. Implementing advanced video capture technology in surveillance areas could alleviate this issue. Here the feature extractor used is C3D resulted low accuracy in the detection which is shown in fig: 1.

5.EXISTING SYSTEM ARCHITECTURE:



Source: UCF Crime Data

Fig 1:Existing System Architecture

The above figure 1 explains about a system for anomaly detection in videos using a combination of a pre-trained 3D Convolutional Neural Network (C3D) for feature extraction and a Multi- Instance Learning (MIL) approach for classification. The system outputs anomaly scores for each video, indicating the overall likelihood of anomalous activity being present.

6.PROPOSED SYSTEM:

The proposed system utilizes Convolutional Neural Networks (CNNs) and the Inflated 3D Convolution (I3D) feature extraction technique for anomaly detection.To simplify, CNNs are a type of deep learning model commonly used for image processing tasks. They work by passing small filters over input images to detect patterns and features.I3D, on the other hand, extends CNNs to video data by incorporating 3D convolutions, which analyze both spatial and temporal information within video frames.In this system, these techniques are combined to extract features from video data effectively. Anomalies, or deviations from normal patterns, are then detected by comparing these extracted features to a model of normal behavior. If the features of a video segment deviate significantly from this model, it is flagged as an anomaly.By using this system the security is high.

7.PROPOSED ARCHITECTURE:

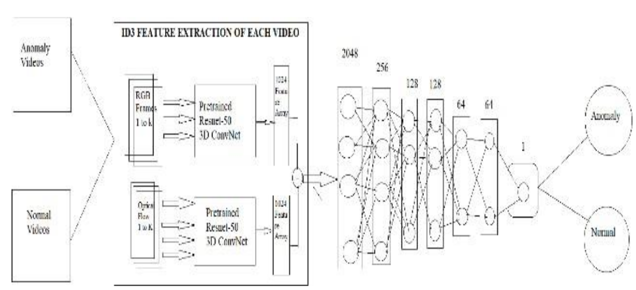


Fig 2a :Proposed system architecture on I3D

Above figure 2a uses two main parts to find unusual activity

Feature extraction: This part takes a video and chops it up into small clips. Then, it uses a special kind of AI model called a3D Convolutional Neural Network (3D ConvNet) to analyzeeach clip and identify important patterns and movementswithin it.

Putting the pieces together: Once the 3D ConvNet has analyzed all the clips, it groups them together based on the The video they came from. The system then tries to figure out if each video contains anything unusual by looking at the patterns it found in the clips. If a video has a clip with patterns that are very different from all the other clips in the same video, then the system flags that video as potentially containing something abnormal.

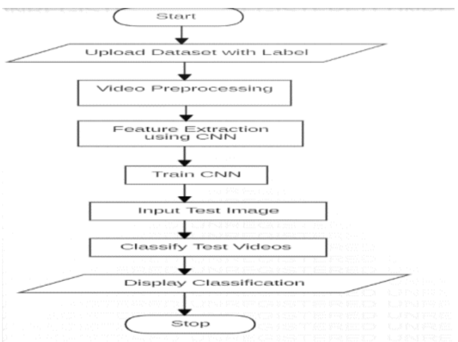


Fig 2b :Proposed system flow chart on CNN

The above fig 2b which shows a flow of video processing for anomaly detection

Start: The process starts with uploading a video with a label (normal or anomaly).

Video Preprocessing: The video is preprocessed to remove noise and prepare it for further analysis.

Feature Extraction using CNN: A type of artificial intelligence called a Convolutional Neural Network (CNN) analyzes the video to extract important features and patterns, like the movement of objects. This is like finding the building blocks of what's happening in the video.

Train CNN: If the video has a label (normal or anomaly), it's used to train the CNN to better identify these types of videos in the future.

Input Test Image: A new video (without a label) is fed into the system.

Classify Test Videos: The CNN uses the extracted features from the test video to classify it as either normal or anomalous. Display Classification: The system displays the classification result (normal or anomaly) for the test video.

Stop: The process ends.

8. ACTIVITY RECOGNITION USING CNN AND I3D FEATURE EXTRACTION

By combining CNNs and I3D for feature extraction, the system can effectively capture both spatial and temporal information from video data. This allows for more accurate recognition of activities, including the detection of anomalies or unusual behavior. Our research strives to create a model capable of automatically recognizing and categorizing actions in videos with a high degree of precision and dependability.

CNNs and I3D feature extraction are like specialized tools that help the system understand what "normal" activity looks like. CNNs are adept at recognizing patterns in images or video frames, while I3D feature extraction enhances this capability by capturing both spatial and temporal information, crucial for understanding motion and activity changes over time.

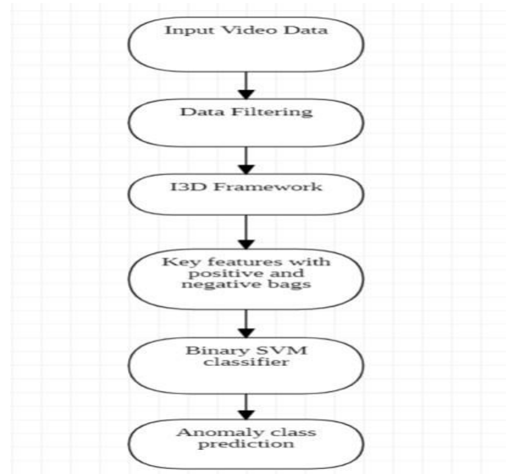


Fig 3 : Overall framework of model

Above fig 3 expiain about depicts the a system for anomaly detection in videos, like security cameras. Frstly,Inputting the Videos are fed into the system. Then, Data Filtering of Videos are filtered to remove noise and irrelevant information.After that I3D Feature Extraction**,** A powerful AI model called I3D analyzes each video clip to identify important patterns and movements, like objects and their motion. Imagine it as finding the building blocks of the video and then Key Features & Bags are the important patterns are grouped together based on whether they're from a normal video (negative bag) or a potentially abnormal video (positive bag).Then next,Binary SVM Classifier, is a special tool called a classifier then analyzes each group of features (bag) to decide if it's likely normal or abnormal.Finally,Anomaly Prediction which helps the system determines the likelihood of each video containing unusual activity based on the analysis of its feature groups.Overall, the system works like a detective, carefully examining videos, identifying important clues, and flagging suspicious ones for further investigation.

9. IMPLENTATION

Problem Definition:

Define the scope and objectives of the anomaly detection task. Specify the types of anomalies you aim to detect and the dataset you will be working with.

Data Collection and Preprocessing:

Gather a dataset containing both normal and anomalous samples.

Preprocess the data to ensure uniformity and compatibility with the neural network models. Images may be resized, pixel values normalized, and the dataset potentially augmented for preprocessing**.**

Feature Extraction with I3D:

Implement the Inflated 3D ConvNet (I3D) model for feature extraction from video data. I3D is a deep learning model pre-trained on large-scale video datasets such as Kinetics.Extract features from both normal and anomalous video sequences using the pre-trained I3D model.

CNN Architecture Design:Design a CNN architecture for anomaly detection. The CNN will take extracted features from the I3D model as input.Consider the number of convolutional layers, pooling layers, and fully connected layers based on the complexity of the dataset.

Model Training:Split the dataset into training, validation, and possibly test sets.Train the anomaly detection model using the training set. Monitor its performance on the validation set to avoid overfitting.Train the CNN model using the extracted features as input and the ground truth labels for supervision.Utilize techniques like cross-validation and regularization to preventoverfitting.

Evaluation:Evaluate the trained model on the test set to assess its performance in detecting anomalies.Utilize confusion matrices or ROC curves to assess the model's ability to differentiate between normal and anomalous samples.

Fine-tuning and Optimization:Fine-tune the model and hyperparameters to improve performance.Experiment with different optimization algorithms, learning rates, and batch sizes to enhance the model's robustness and generalization ability.

Deployment and Monitoring:

Deploy the trained model for real-time or batch anomaly detection in a production environment.Implement monitoring mechanisms to track the model's performance and retrain it periodically with new data if necessary.

Embed the trained model into your chosen application/system for real-time or batch anomaly detection.Continuously monitor the model's performance and retrain it if necessary to adapt to new data and maintain accuracy.

10. RESULT AND DISCUSSION

Sample code for normal,abnormal and emergency conditions:

```
# print(predaction[1])
cv2.putText(frame,
    'Normal ',
    (50, 50),
    font, 2,
    (100, 125, 255),
    3,
    cv2.LINE_4)
cv2.imshow('Normal ', frame)
# time.sleep(1)
print('Normal  here ...')
```

Fig 4A

```
if predaction[0] == True:
    # print(predaction[1])
    cv2.imwrite('output/abnormal.jpg', frame)
    cv2.putText(frame,
        'Abnormal Detected',
        (50, 50),
        font, 2,
        (0, 255, 255),
        3,
        cv2.LINE_4)
    mail("EMERGENCY_HELP")
    # time.sleep(1)q
    cv2.imshow('abnormal Detected', frame)
    print('abnormal detected here ...')
```

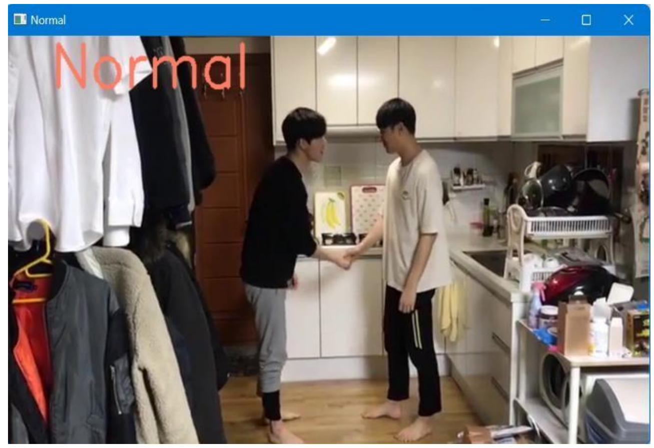
Fig 4B

```
fromaddr="nandhunaidu16@gmail.com"

toaddr="bjyoshnapriya@gmail.com"

def mail(text):
    print(text)
    msg=MIMEMultipart()
    msg['From']=fromaddr
    msg['To']=toaddr
    msg['Subject']="EMERGENCY_HELP"
    body=text
    msg.attach(MIMEText(body,'plain'))
    filename="output/abnormal.jpg"
    attachment=open("output/abnormal.jpg","rb")
```

Fig 4C



. Fig 4A : Normal Detection

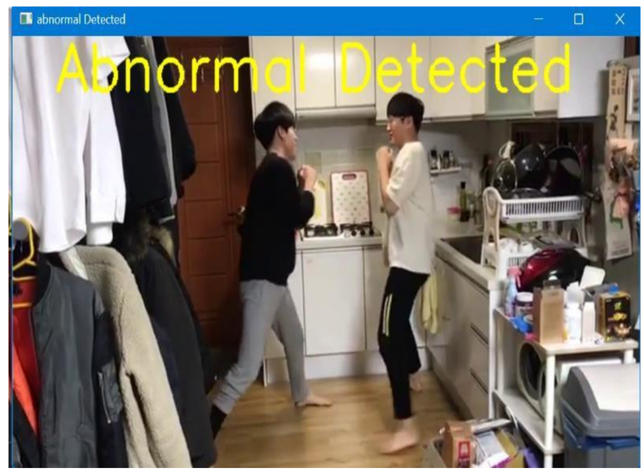


Fig 4B :Abnormal Detection

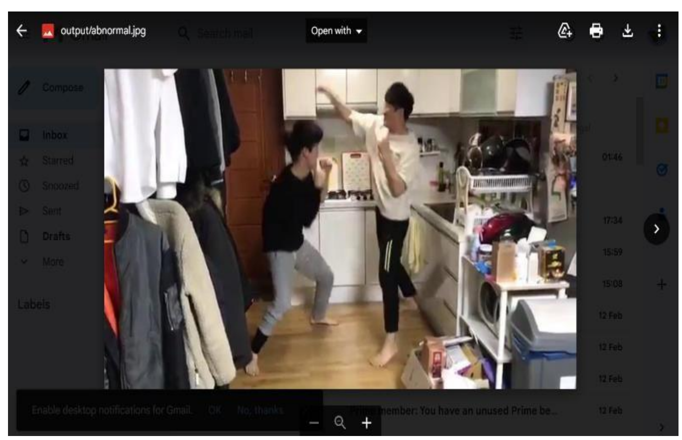


Fig 4C:Emergency help

SAMPLE TERMINAL OUTPUT:

```
model loaded from: myWeights.hdfs
1/1 [==============================] - 3s 3s/step
Normal  here ...
1/1 [==============================] - 2s 2s/step
Normal  here ...
1/1 [==============================] - 2s 2s/step
Normal  here ...
1/1 [==============================] - 3s 3s/step
Normal  here ...
1/1 [==============================] - 3s 3s/step
EMERGENCY_HELP
abnormal detected here ...
1/1 [==============================] - 3s 3s/step
EMERGENCY_HELP
abnormal detected here ...
1/1 [==============================] - 3s 3s/step
EMERGENCY_HELP
abnormal detected here ...
end of the video
```

Fig 4: Terminal code

CONCLUSION

This study explored the synergy between Convolutional Neural Networks (CNNs) and I3D feature extraction for video anomaly detection. The proposed approach exhibited significant accuracy gains compared to conventional methods, particularly in challenging scenarios characterized by complexity and crowd density. These findings highlight the potential of this technique for real-world applications.However, several key challenges warrant further investigation. The model's performance hinges on access to voluminous and diverse video datasets, posing potential resource constraints. Additionally, achieving interpretability in these deep learning models remains an ongoing challenge, limiting our understanding of the specific patterns driving anomaly detection. Finally, fine-tuning the model for specific domains and applications might be necessary to maximize its effectiveness.Addressing these data, interpretability, and domain adaptation challenges through continued research holds immense promise. By overcoming these hurdles, we can unlock the full potential of CNN-I3D based anomaly detection and pave the way for its wider adoption across diverse real-world domains. This research could revolutionize anomaly detection, leading to safer systems, enhancing security, efficiency, more accurate predictions and overall safety in various applications.

REFERENCES

1. S. Shashikar and V. Upadhyaya, "Traffic surveillance and anomaly detection using image processing," *2017 Fourth International Conference on Image Information Processing (ICIIP)*, Shimla, India, 2017, pp. 1-6, doi: 10.1109/ICIIP.2017.8313721.
2. S. Gunduz, U. Yavanoglu and S. Sagiroglu, "Predicting Next Location of Twitter Users for Surveillance," *2013 12th International Conference on Machine Learning and Applications*, Miami, FL, USA, 2013, pp. 267-273, doi: 10.1109/ICMLA.2013.134.
3. Anuar, S., Selamat, A., & Sallehuddin, R. (2015). Hybrid artificial neural network with artificial bee colony algorithm for crime classification. In *Computational Intelligence in Information Systems: Proceedings of the Fourth INNS Symposia Series on Computational Intelligence in Information Systems (INNS-CIIS 2014)* (pp. 31-40). SpringerInternational Publishing.
4. Azeez, J., & Aravindhar, D. J. (2015, August). Hybrid approach to crime prediction using deep learning. In *2015 International Conference on Advances in Computing, Communications and Informatics (ICACCI)* (pp. 1701-1710). IEEE.
5. M. Saravanan, R. Thayyil and S. Narayanan, "Enabling Real Time Crime Intelligence Using Mobile GIS and Prediction Methods," *2013 European Intelligence and Security Informatics Conference*, Uppsala, Sweden, 2013, pp. 125- 128, doi: 10.1109/EISIC.2013.27.
6. Lin, Y. L., Chen, T. Y., & Yu, L. C. (2017, July). Using machine learning to assist crime prevention. In *2017 6th IIAI international congress on advanced applied informatics (IIAI-AAI)* (pp. 1029-1030). IEEE.
7. Irfan, M., Tokarchuk, L., Marcenaro, L., & Regazzoni, C. (2018, November). Anomaly detection in crowds using multi sensory information. In *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)* (pp. 1-6). IEEE.
8. Yang, Jing & Eickhoff, Carsten. (2017). Unsupervised Spatio-Temporal Embeddings for User and Location Modelling.
9. Bose, B., Dutta, J., Ghosh, S., Pramanick, P., & Roy, S. (2018, February). D&RSense: Detection of driving patterns and road anomalies. In *2018 3rd International Conference On Internet of Things: Smart Innovation and Usages (IoT- SIU)* (pp. 1-7). IEEE.
10. Nakib, M., Khan, R. T., Hasan, M. S., & Uddin, J. (2018, February). Crime scene prediction by detecting threatening objects using convolutional neural network. In *2018 international conference on computer, communication, chemical, material and electronic engineering (IC4ME2)* (pp. 1-4). IEEE.
11. P. Yang, W. Jin and P. Tang, "Anomaly Detection of Railway Catenary Based on Deep Convolutional Generative Adversarial Networks," *2018 IEEE 3rd Advanced Information Technology, Electronic and Automation Control Conference (IAEAC)*, Chongqing, China, 2018, pp. 1366- 1370, doi: 10.1109/IAEAC.2018.8577821.
12. Wang, B., Yin, P., Bertozzi, A.L. *et al.* Deep Learning for Real-Time Crime Forecasting and Its Ternarization. *Chin. Ann. Math. Ser. B* **40**, 949–966 (2019). https://doi.org/10.1007/s11401-019-0168-y.
13. Y. Qin and Y. Lou, "Hydrological Time Series Anomaly Pattern Detection based on Isolation Forest," *2019 IEEE 3rd Information Technology, Networking, Electronic and Automation Control Conference (ITNEC)*, Chengdu, China, 2019, pp. 1706-1710, doi: 10.1109/ITNEC.2019.8729405.
14. Gahalot, A., Dhiman, S., & Chouhan, L. (2020, February). Crime prediction and analysis. In *2nd International Conference on Data, Engineering and Applications (IDEA)* (pp. 1-6). IEEE.
15. Rajapakshe, C., Balasooriya, S., Dayarathna, H., Ranaweera, N., Walgampaya, N., & Pemadasa, N. (2019, December). Using cnns rnns and machine learning algorithms for real-

time crime prediction. In *2019 International Conference on Advancements in Computing (ICAC)* (pp. 310-316). IEEE.

16. S. Sathyadevan, M. S. Devan and S. S. Gangadharan, "Crime analysis and prediction using data mining," *2014 First International Conference on Networks & Soft Computing (ICNSC2014)*, Guntur, India, 2014, pp. 406-412, doi: 10.1109/CNSC.2014.6906719.
17. N. Mahmud, K. I. Zinnah, Y. A. Rahman and N. Ahmed, "Crimecast: A crime prediction and strategy direction service," *2016 19th International Conference on Computer and Information Technology (ICCIT)*, Dhaka, Bangladesh, 2016, pp. 414-418, doi:10.1109/ICCITECHN.2016.7860234.
18. Nakib, M., Khan, R. T., Hasan, M. S., & Uddin, J. (2018, February). Crime scene prediction by detecting threatening objects using convolutional neural network. In *2018 international conference on computer, communication, chemical, material and electronic engineering (IC4ME2)* (pp. 1-4). IEEE.
19. M. Irfan, L. Tokarchuk, L. Marcenaro and C. Regazzoni, "ANOMALY DETECTION IN CROWDS USING MULTI SENSORY INFORMATION," *2018 15th IEEE International Conference on Advanced Video and Signal Based Surveillance (AVSS)*, Auckland, New Zealand, 2018, pp. 1-6, doi: 10.1109/AVSS.2018.8639151.
20. Almaw, A., & Kadam, K. (2018). Survey paper on crime prediction using ensemble approach. *International Journal of Pure and Applied Mathematics*, *118*(8), 133-139.
21. S. Kim, P. Joshi, P. S. Kalsi and P. Taheri, "Crime Analysis Through Machine Learning," *2018 IEEE 9th Annual Information Technology, Electronics and Mobile Communication Conference (IEMCON)*, Vancouver, BC,Canada, 2018, pp. 415-420, doi:10.1109/IEMCON.2018.8614828.