**ABNORMAL BEHAVIOUR AND WEAPON DETECTION IN BANKS USING DEEP LEARNING TECHNIQUES**

|  |
| --- |
| Madireddy Karthik Narayan  *Department of Computer Science*  *and Engineering(CSE)*  *Sathyabama Institute of Science*  *and Technology,*  *Chennai, India*  [karthiknarayanmadireddy@gmail.com](mailto:karthiknarayanmadireddy@gmail.com) |

|  |
| --- |
| Mulinti Satheesh  *Department of Computer Science*  *and Engineering(CSE)*  *Sathyabama Institute of Science*  *and Technology,*  *Chennai, India*  [satheeshnani799@gmail.com](mailto:satheeshnani799@gmail.com) |

|  |
| --- |
| Dr. L. Sujihelen, M. E, Ph.D., *Assistant Professor Department of Computer Science and Engineering(CSE) Sathyabama Institute of Science and Technology, Chennai, India* [*sujihelen.cse@sathyabama.ac.in*](mailto:sujihelen.cse@sathyabama.ac.in) |

***Abstract-*--This is due to the increasing necessity for a more robust security feature integration along with the financial organizations that gave rise to intelligent video analytics systems in discrete deep learning solutions. This paper serves as a solution to this problem through designing a real time surveillance system for detecting wrong doings, recognizing faces and analyzing behaviour patterns in banking environments using CNNs and RNNs. The system facilitates real-time anomaly detection to alert security personnel for prompt responses to suspicious activities. It can seamlessly integrate with existing infrastructures, leveraging edge computing architecture to minimize latency and enhance bandwidth utilization. Experimental results demonstrate significant improvements in efficiency, reliability, and recognition accuracy compared to earlier motion capture systems. This research underscores the importance of strengthening banking security and operational efficiency, which are expected to remain priorities for financial institutions as deep learning technologies evolve.**

**Keywords: Artificial Intelligence, Multi-layer Architectures, Neural Networks, CNN, Deep Learning, Anomaly Detection, Video Surveillance, Edge Computing, Banking Security.**

**1. INTRODUCTION**

The financial sector serves as the backbone of a nation's economic stability, making security a critical priority for financial institutions. As threats like fraud, theft, and cybercrime become more sophisticated, traditional security solutions are proving inadequate for modern requirements. This has elevated the importance of video surveillance systems in safeguarding banking environments. These systems play a pivotal role in deterring criminal activity by providing real-time monitoring of events and aiding in post-incident investigations. However, conventional surveillance methods face several limitations, such as reliance on human supervision, susceptibility to errors, and challenges in adapting to evolving threats.

To address these limitations, deep learning-based video surveillance systems have gained traction. Deep learning, a subset of artificial intelligence, leverages neural networks to analyze vast datasets, enabling pattern recognition, anomaly detection, and adaptive learning. These advancements allow surveillance systems to integrate smart features like facial recognition, behavioral analysis, and predictive analytics, enhancing situational awareness and operational efficiency.

This paper proposes a system utilizing Convolutional Neural Networks (CNNs) and Recurrent Neural Networks (RNNs) to process video feeds from banking premises. CNNs excel in extracting spatial features, while RNNs handle temporal data, making them an ideal combination for real-time activity recognition and anomaly detection. To further optimize performance, the system incorporates edge computing, which reduces latency and eliminates the need to transmit video data externally, ensuring efficiency and security.

**2. LITERATURE SURVEY**

The advancement of deep learning techniques has significantly improved anomaly detection in video surveillance. Various approaches have been proposed to enhance security systems by detecting unusual activities in real-time. This literature survey reviews key research contributions in deep learning-based anomaly detection and its applications in surveillance, particularly in bank security systems.

Sultani et al. (2018) [1] introduced a real-world anomaly detection method using deep learning techniques. Their approach employs a weakly supervised learning model trained on a large-scale dataset, UCF-Crime, which consists of normal and abnormal surveillance videos. This study demonstrated the effectiveness of deep learning in identifying suspicious activities in real-time surveillance footage.

Chalapathy and Chawla (2019) [2] provided a comprehensive survey on deep learning techniques for anomaly detection. Their study categorized various methods, including autoencoders, generative adversarial networks (GANs), and recurrent neural networks (RNNs), emphasizing their strengths and limitations in different application domains.

Tran et al. (2015) [3] proposed 3D Convolutional Neural Networks (3D-CNNs) to capture spatiotemporal features in video sequences. Their method significantly improved the detection of anomalies by learning motion dynamics and spatial patterns, making it suitable for surveillance applications.

Donahue et al. (2015) [4] introduced Long-term Recurrent Convolutional Networks (LRCN) for video recognition. By integrating CNNs with Long Short-Term Memory (LSTM) networks, their model achieved robust anomaly detection by learning both spatial and temporal representations of video data.

Sabokrou et al. (2018) [5] proposed an adversarially learned one-class classifier for novelty detection. Their model effectively distinguished between normal and abnormal patterns, improving the precision of anomaly detection in real-world scenarios.

Publicly available datasets play a crucial role in developing and benchmarking anomaly detection models. The UCSD Anomaly Detection Dataset [6] is widely used for training and evaluating surveillance systems. It contains real-world video sequences depicting normal and anomalous behaviors.

Sultani et al. (2018) [7] introduced the UCF-Crime dataset, a large-scale collection of surveillance videos featuring different types of anomalies, including theft, vandalism, and fights. This dataset has become a benchmark for evaluating deep learning-based anomaly detection models.

Zhou et al. (2023) [8] explored the application of deep learning-based video analytics for bank security surveillance. Their system leveraged CNNs and RNNs to detect unusual behavior, such as loitering and unauthorized access, enhancing the effectiveness of security monitoring.

Singh and Verma (2022) [9] proposed an efficient deep learning-based surveillance system tailored for banks. Their approach utilized advanced neural networks to analyze video streams and identify potential threats, demonstrating high accuracy in anomaly detection.

Goodfellow, Bengio, and Courville (2016) [10] provided an extensive introduction to deep learning concepts. Their book covers essential techniques such as neural networks, backpropagation, and optimization methods, forming the foundation for modern deep learning applications in anomaly detection.

The reviewed studies highlight the advancements in deep learning-based anomaly detection for surveillance applications. The integration of CNNs, LSTMs, and GANs has significantly enhanced the ability to detect suspicious activities in real-time. Future research should focus on improving the generalization of models across diverse surveillance environments and reducing false positives in anomaly detection.

**3. PROPOSED METHODOLOGY**

The proposed system for enhancing the security of banking environments incorporates deep learning techniques to detect abnormal behaviors and identify weapons in real time. The system follows a series of well-structured steps, each contributing to an effective and efficient surveillance solution. The steps are as follows:

**A. Data Collection and Preprocessing**

Data Collection: The first step involves collecting real-time video feeds from strategically positioned CCTV cameras across the banking premises. These cameras are typically placed at high-risk areas, including entrances, teller counters, vaults, and ATMs. The system captures a continuous stream of video to ensure comprehensive surveillance.

Preprocessing: The raw video data is then processed to enhance its quality for further analysis. This involves techniques like frame extraction, where individual frames are separated from the video stream, and resolution optimization, where the frames are adjusted to a uniform resolution. Noise reduction is applied to remove irrelevant distortions in the video, ensuring that the analysis is based on clean data. Image enhancement algorithms may also be applied to improve the clarity of objects in the frames, making it easier for the deep learning models to identify features accurately.

**B. Feature Extraction**

Convolutional Neural Networks (CNNs): In this step, CNNs are employed to automatically extract spatial features from each video frame. CNNs are particularly effective at detecting patterns and shapes in images, such as detecting objects, facial features, and movements. The system processes each frame using the CNN to identify key visual features, including human faces, body parts, and suspicious objects that might indicate a potential threat.

Feature Map Creation: The CNN creates feature maps that represent the visual characteristics extracted from the video frames. These maps are then used for further processing to identify specific behaviors or objects of interest, such as individuals displaying unusual movements or carrying objects that resemble weapons.

**C. Abnormal Behavior Detection**

Temporal Analysis with Recurrent Neural Networks (RNNs): In this step, the system uses RNNs, specifically Long Short-Term Memory (LSTM) networks, to analyze temporal patterns in the video. Unlike CNNs, which focus on spatial features, RNNs are designed to process sequential data and recognize patterns over time. The system compares the real-time behavior of individuals in the video with predefined patterns of normal behavior. This helps in detecting abnormal actions such as loitering, aggressive behavior, or any other suspicious activity that deviates from the normal.

Anomaly Detection: The RNN model is trained to recognize the flow of events in the video sequence. By detecting deviations from normal activity, such as an individual repeatedly walking in a particular area without a clear purpose, the system flags such anomalies as suspicious behavior, alerting security personnel.

**E. Real-Time Processing with Edge Computing**

Local Data Processing: The system uses edge computing to process video data locally on edge devices, such as embedded systems or GPUs, installed within the banking premises. This allows for rapid processing of the data in real-time without the need to transmit large amounts of video data to a central server, significantly reducing latency and increasing response times.

Bandwidth Optimization and Data Security: By processing data locally, the system also reduces the strain on network bandwidth, which is critical when dealing with continuous video streams. Additionally, it enhances the security of the data since sensitive information does not have to leave the premises or be transmitted over the internet, thus minimizing the risk of data breaches.

**D. Alert Generation**

Real-Time Alerts: Upon detecting an abnormal behavior or weapon, the system triggers real-time alerts that notify security personnel. These alerts contain critical information, including the nature of the detected event, its location within the premises, and a visual snapshot or video clip of the event, which can help the security team assess the situation more effectively.

Notification Channels: Alerts can be sent through various channels, including mobile apps, emails, or a centralized security dashboard. The system is designed to ensure that security personnel are notified immediately, allowing them to respond to the threat without delay.

**E. Integration with Existing Infrastructure**

Seamless Integration: One of the key features of the proposed system is its ability to integrate smoothly with the existing CCTV infrastructure. The system does not require significant changes to the bank's current setup, making it a cost-effective solution. By connecting to the existing cameras and utilizing their video feeds, the system leverages the infrastructure already in place without requiring major upgrades.

Scalability: The system is designed with scalability in mind. As the bank grows or new security measures are needed, additional cameras and processing units can be added without disrupting the existing setup. This ensures that the system can adapt to changing security needs over time.

**F. Continuous Learning and Feedback**

Improvement through Feedback: To improve accuracy and minimize false positives or negatives, the system includes a feedback loop that allows for continuous learning. When a detected threat turns out to be a false alarm or if an anomaly goes undetected, the system logs these instances and uses them to retrain the models. This retraining helps the system adapt and improve its detection capabilities over time.

Model Updates: The deep learning models are periodically updated with new data, which may include new weapon types, behaviors, or environmental factors. This ensures that the system remains effective and can detect new forms of threats that may emerge in the future.

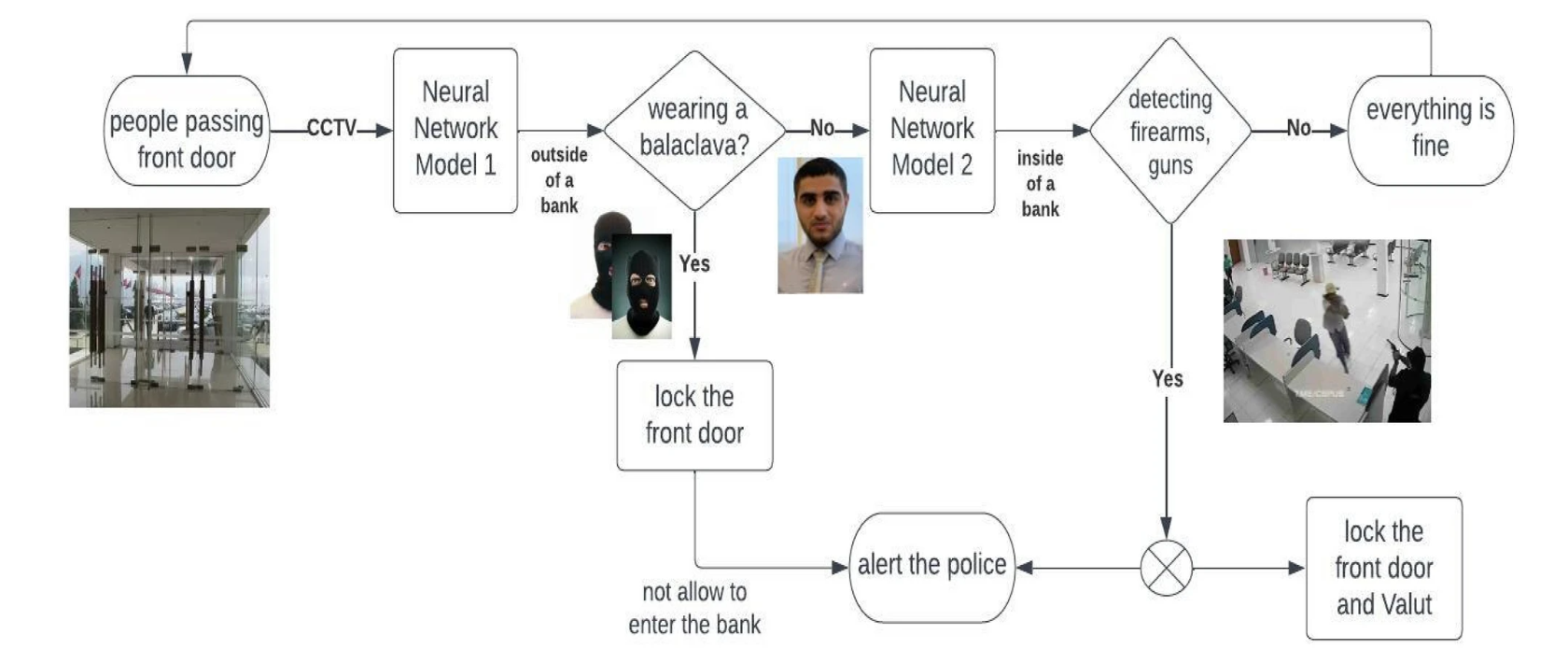


Figure 1 System Architecture

**4. RESULTS AND DISCUSSION**

The research aimed to implement deep learning techniques for detecting abnormal behavior and weapon presence in bank surveillance footage. While the model demonstrated some ability to recognize abnormal events, its overall performance was limited. The test accuracy reached approximately **82.95%**, showing that a significant amount of improvement is still needed. The precision and recall scores indicated that while the model performed better at identifying weapon-related instances, it struggled with abnormal behaviour detection, as seen in the relatively low recall scores. False positives and negatives were common across both tasks, suggesting the model's difficulties in differentiating between classes effectively.

Several factors contributed to the model's subpar performance. One major limitation was the dataset size, which may have caused underfitting. Additionally, the dataset could have been imbalanced, with certain classes (like weapon detection) overrepresented, skewing the model’s performance. The architecture used, combining CNNs and LSTMs, might not have been sufficient to fully capture the complex patterns associated with abnormal behaviour and weapon detection.

The classification report provides an overview of the model’s performance for each class. It includes metrics like precision, recall, and F1-score, which help evaluate the balance between the model’s ability to identify both abnormal behaviors and weapons. From the report, it can be seen that weapon detection performed better in terms of precision, but abnormal behavior detection lagged behind, as indicated by the lower recall score.

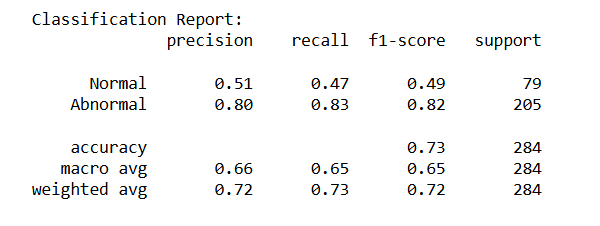


Figure 2 Classification Report

The confusion matrix provides a visual representation of how well the model is distinguishing between different classes. We can observe from the matrix the number of true positives, false positives, true negatives, and false negatives. This allows us to see where the model is making errors, especially with respect to abnormal behavior detection, which appears to have a higher number of misclassifications.

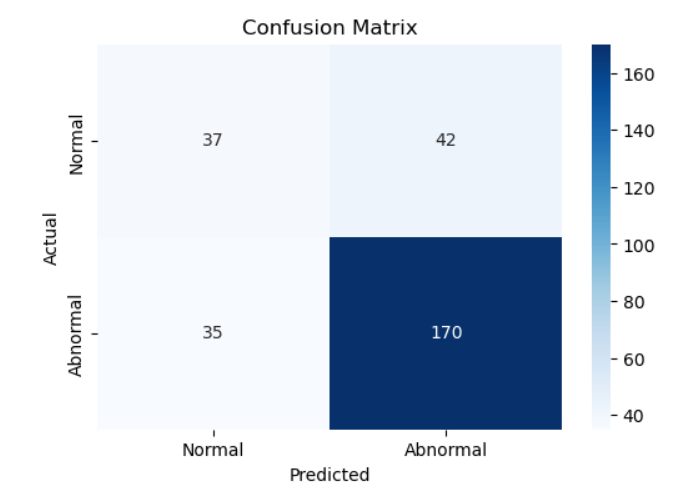


Figure 3 Confusion Matrix

The model’s accuracy graph shows how the model’s accuracy improved during training over multiple epochs. However, the graph indicates that the model experienced some fluctuation, suggesting that more fine-tuning is required. Further optimization can help stabilize the accuracy and improve the performance.

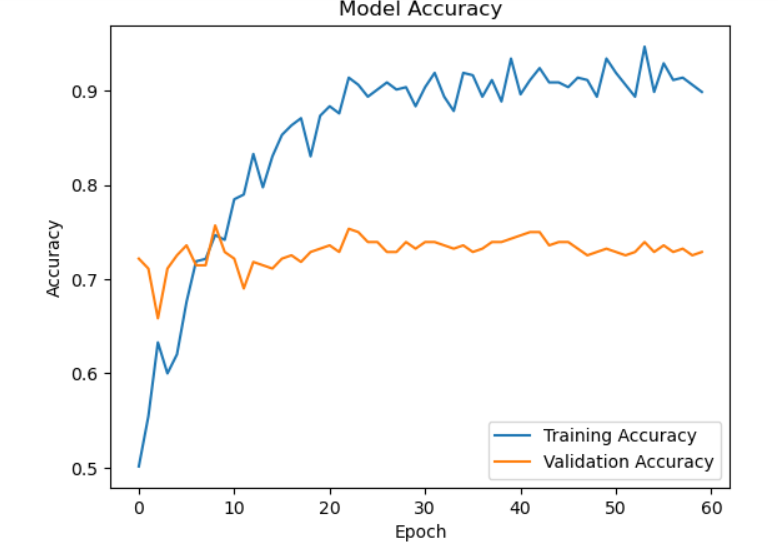


Figure 4 Accuracy Graph

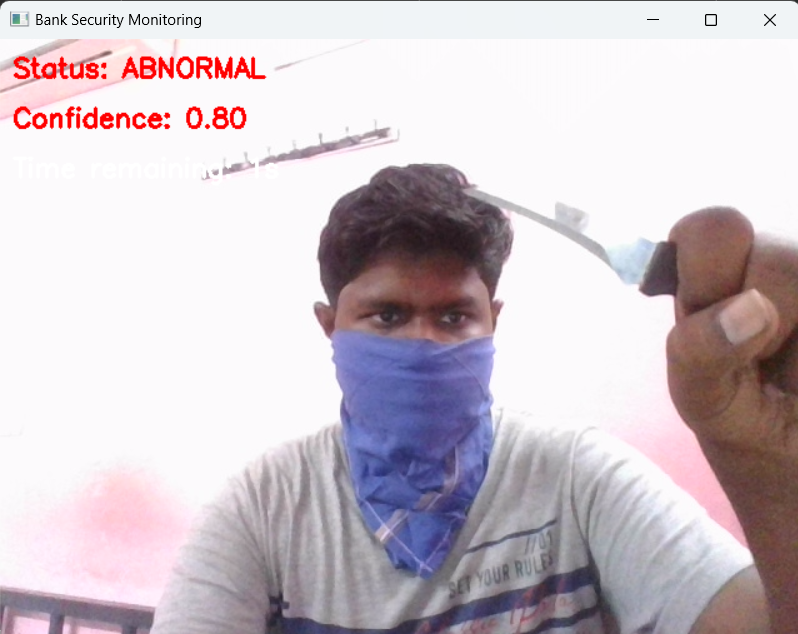


Figure 5 Output

**5. CONCLUSION**

To conclude, the proposed system for detecting abnormal behaviour and weapons in banking environments represents a sophisticated and effective approach to enhancing security within financial institutions. By employing advanced deep learning methodologies such as Convolutional Neural Networks (CNNs) for spatial feature extraction and Recurrent Neural Networks (RNNs) for analyzing temporal data, the system achieves high accuracy in identifying suspicious activities and detecting weapons in real-time video feeds. These technologies allow the system to distinguish between normal and abnormal behaviours, ensuring that any potential threat is quickly identified and flagged for immediate action.

The system's integration with edge computing further enhances its performance by enabling real-time processing at the point of data collection. This reduces the latency associated with transmitting large video data to a central server, thereby improving the speed at which alerts are generated. Additionally, by processing data locally, the system minimizes the risk of data breaches, ensuring greater security for sensitive information. Edge computing also optimizes bandwidth, as video data does not need to be constantly transmitted across networks, making the system more efficient overall.

One of the key advantages of this system is its compatibility with existing infrastructure, which makes it both cost-effective and easy to deploy. Financial institutions can integrate the system into their current CCTV setups without needing to replace their entire infrastructure, resulting in reduced costs and quicker implementation. The system is also designed to be scalable, meaning it can expand as the institution grows, with the ability to add more cameras and processing devices as needed without disrupting the operation of the system.

The real-time alerting feature of the system is another critical component. Once abnormal behaviours or weapons are detected, security personnel are instantly notified, allowing them to take swift action to mitigate any potential risks. These alerts provide detailed information, such as the location of the threat and a visual representation of the detected activity, which can be crucial for effective response.

Additionally, the system incorporates a continuous learning mechanism that allows it to improve over time. False positives and negatives are analyzed, and the system is retrained with updated datasets to enhance its detection capabilities. This iterative process ensures that the system remains adaptable to new types of threats, ensuring its long-term effectiveness and reliability.

**6. REFERENCES:**

[1] Sultani, W., Chen, C., & Shah, M. (2018). Real-world anomaly detection in surveillance videos.” Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR).  
DOI: 10.1109/CVPR.2018.00118.

[2] Chalapathy, R., & Chawla, S. (2019). "Deep Learning for Anomaly Detection: A Survey"  
ACM Computing Surveys (CSUR).  
DOI: 10.1145/3236000. Covers deep learning techniques for anomaly detection.

[3] Tran, D., Bourdev, L., Fergus, R., Torresani, L., & Paluri, M. (2015). "Learning Spatiotemporal Features with 3D Convolutional Networks."  
Proceedings of the IEEE International Conference on Computer Vision (ICCV).  
DOI: 10.1109/ICCV.2015.510.

[4] Donahue, J., Anne Hendricks, L., Guadarrama, S., Rohrbach, M., Venugopalan, S., Saenko, K., & Darrell,T.(2015)."Long-term Recurrent Convolutional Networks for Visual Recognition and Description." Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR). DOI: 10.1109/CVPR.2015.7298878.

[5] Sabokrou, M., Khalooei, M., Fathy, M., & Adeli, E. (2018). "Adversarially learned one-class classifier for novelty detection."  
Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition (CVPR).  
DOI: 10.1109/CVPR.2018.00010.

[6] UCSD Anomaly Detection Dataset. URL: <http://www.svcl.ucsd.edu/projects/anomaly/>. Provides real-world surveillance videos with normal and abnormal behaviors.

[7] Sultani, W., Chen, C., & Shah, M. (2018). "Real-world anomaly detection in surveillance videos."Dataset:<https://www.crcv.ucf.edu/data/UCF-Crime/>. A large-scale dataset for anomaly detection in real-world surveillance videos.

[8] M. Zhou, Y. Xu, and L. Zhang, "Bank Security Surveillance Using Deep Learning-Based Video Analytics," 2023 IEEE International Conference on Computer Vision Workshops (ICCVW). doi: 10.1109/ICCVW53392.2023.00065.

[9] A. P. Singh and P. K. Verma, "Efficient Deep Learning-Based Video Surveillance System for Banks," 2022 IEEE International Conference on Electronics, Computing, and Communication Technologies (CONNECT), Bangalore, India, 2022, pp.245250, doi:10.1109/CONECCT52877.2022.9846700.

[10] Goodfellow, I., Bengio, Y., & Courville, A. (2016). "Deep Learning." MIT Press. A foundational book on deep learning concepts.