WWW.IJRPR.COM

International Journal of Research Publication and Reviews

Journal homepage: www.ijrpr.com ISSN 2582-7421

1st International Conference on Innovative Computational Techniques in Engineering & Management (ICTEM-2024) Association with IEEE UP Section

Real-Time Intrusion Detection for Home Security: Using Machine Learning

Mr. Vinay K. Pant[1], Ms. Bindu Rani[2], Naman Sharma[3], Anshika Bhatnagar[4], Mohd. Mudassir[5], Arzan Hussain[6]

[1,2]Assistant Professor Department of Computer Science and Engineering (AIML) Moradabad Institute of Technology Moradabad
[1]pantvinay02@gmail.com [2]binducs026@gmail.com
[3,4,5,6]Department of Computer Science and Engineering (AIML), Moradabad Institute of Technology, Moradabad
3n.sharma9561@gmail.com 4bhatnagaranshika17@gmail.com 5mdmudassir5019@gmail.com 6arzanhussain7505@gmail.com

DOI: https://doi.org/10.55248/gengpi.6.sp525.1933

Abstract:

This is the time of the advancement of technology. Here every day new automated technology comes in the market. We are using these technologies in our day-to-day life and industrial advancement. But some time we are facing some issues that are till now unsolved or partially solved. In this paper we are working on one of the security issues. The "Real-Time Intrusion Detection" system presents an advanced security solution utilizing the synergy of image processing technology, ML techniques, and artificial intelligence to enhance monitoring systems. The system is designed to recognize known faces, detect the presence of unknown individuals, analyze sentiment, and identify potential threats, including weapons, in real time. The research aims to improve the responsiveness and efficiency of security protocols by providing live updates, including images of suspicious individuals, to security personnel. This innovative solution could greatly enhance safety and situational awareness in sensitive areas such as airports, banks, and corporate offices by automating threat detection and decision-making processes.

Keywords: ***Artificial Intelligence, Machine Learning, Face Detection, Intruders, Home Security System.***

1. Introduction

The "Real-Time Intrusion Detection" system is an innovative and multifaceted security solution that leverages cutting-edge technologies such as image processing technology, ML techniques (ML), and artificial intelligence (artificial intelligence). It is designed to identify individuals, detect new faces, analyze sentiment, and recognize potential threats, including weapons, thereby providing immediate monitoring and ensuring safety. The system also updates users with images of suspicious individuals, improving the responsiveness and efficiency of security protocols Agustina J. R. and Clavell G (2019). This paper reviews and critically analyzes existing research on this topic, highlighting key technological advancements, methodologies, challenges, and future directions in immediate intrusion detection.

2. Literature Review

The field of immediate intrusion detection using image processing technology and artificial intelligence has witnessed significant advancements in recent years, with growing interest in security solutions for high-risk environments. Studies have demonstrated the effectiveness of deep learning techniques in face recognition. For instance, Schroff et al. (2015) introduced FaceNet, a deep learning model that achieved unprecedented accuracy in recognizing individuals across various datasets. Similarly, Taigman et al. (2014) developed the DeepFace model, which leveraged deep neural networks to surpass human-level performance in face recognition tasks.

In terms of anomaly detection, One-Class SVMs have been widely used for detecting outliers in monitoring systems. A study by Ahmed et al. (2016) employed one-class SVMs for anomaly detection in video monitoring, achieving significant improvements in identifying suspicious behavior. Further, k-means clustering and Gaussian Mixture Models (GMM) have been employed to identify individuals who do not fit normal patterns in immediate scenarios.
Weapon detection has also been extensively researched in the context of monitoring systems. Redmon et al. (2016) introduced YOLO, a immediate

object detection algorithm that excelled at identifying various objects, including weapons, with high speed and accuracy. Other approaches, such as Faster R-CNN (Ren et al., 2015), have been employed for object detection, providing a balance between speed and precision.

Sentiment analysis and emotion recognition using image processing technology are relatively newer domains but have shown promise. Studies by Zhang et al. (2020) used deep learning models for facial expression recognition, demonstrating the system's ability to analyze sentiment from video data in real time, thus adding another layer of threat assessment to security systems.

This growing body of research underpins the "Real-Time Intrusion Detection" project, which seeks to combine the advancements in face recognition, anomaly detection, and weapon identification into a cohesive immediate system.

3. Proposed Methodology

3.1. Data Collection and Preprocessing

To develop a robust immediate intrusion detection system, the first step involves the collection of diverse datasets. We will gather large datasets comprising images of known and unknown individuals, as well as labelled data representing various objects, including weapons and non-threatening items. The preprocessing of the collected data is crucial for model performance. This will include:

3.1.1. Resizing: Images will be resized to standard dimensions to ensure uniformity across the dataset.

3.1.2. Normalization: Pixel values will be normalized to a range suitable for training deep learning models, typically [0, 1].

3.1.3. Augmentation: To enhance the diversity and generalization of the models, we will employ data augmentation techniques such as rotation, flipping, and brightness adjustments.

3.2. Face Recognition Module

We will implement a facial recognition system utilizing advanced deep learning models, particularly:

3.2.1. Convolutional Neural Networks (CNNs): This architecture will be employed for feature extraction from face images.

3.2.2. Transfer Learning: We will leverage pre-trained models such as VGG-Face and FaceNet to enhance accuracy in immediate face identification. Transfer learning allows us to utilize existing knowledge from these models, improving performance while reducing training time.

3.3. Anomaly Detection (New Individuals)

To identify individuals who do not match known profiles, we will develop an anomaly detection algorithm utilizing:

3.3.1. Clustering Techniques: Employ clustering algorithms to group known faces, facilitating the identification of unknown individuals.

3.3.2. One-Class Support Vector Machines (SVMs): This method will be implemented to flag unknown individuals for further analysis based on their features.

Additionally, we will utilize feature extraction techniques such as Histogram of Oriented Gradients (HOG) and Scale-Invariant Feature Transform (SIFT), combined with classifiers like SVM and K-Nearest Neighbors (KNN) to identify new or suspicious individuals effectively.

3.4. Sentiment Analysis

To assess potential threats through emotional cues, we will utilize image processing technology-based emotion recognition models, such as:

3.4.1. OpenFace: This model will analyze facial expressions to detect emotions in real time.

Moreover, if textual data is available, we will perform sentiment analysis by integrating visual and text- based insights to determine whether a person's expression indicates a threat or normal behaviour.

3.5. Weapon Detection

For detecting weapons, we will implement state-of-the-art object detection algorithms including:

YOLO (You Only Look Once): This algorithm will facilitate the rapid identification of weapons in live video feeds.

Faster R-CNN: This model will be trained using specific datasets of weapons to classify suspicious activities and generate alarms for potential threats.

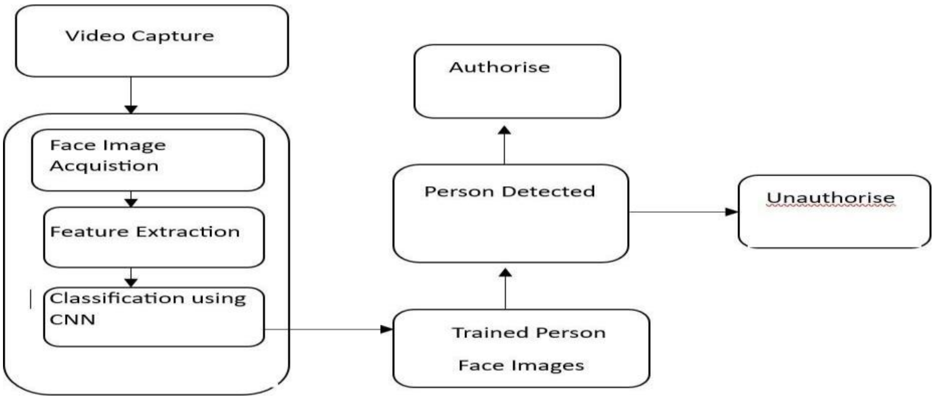

Figure 1 Architecture of Intrusion Detection

3.6. System Integration and Real-Time Monitoring

The various modules will be integrated into a unified platform capable of analyzing live video feeds. The system will employ:

APIs or Message-Passing Systems: These will be utilized to alert security personnel in real time when anomalies are detected, providing visual proof (images) to support assessments.

Real-Time Testing: Extensive testing will be conducted across different environments to ensure the system's robustness and accuracy.

3.7. Performance Evaluation and Refinement

To ensure the efficacy of the proposed system, we will assess its performance using several metrics, including:

Accuracy: Measure the percentage of correctly identified instances.

Precision and Recall: Evaluate the model's performance in terms of false positives and false negatives.

F1 Score: Calculate the harmonic mean of precision and recall to assess overall performance.

Stress testing will be conducted under varying lighting conditions and environmental factors to refine model performance and minimize false positives or negatives. Continuous iteration and enhancement of the models will be performed based on the evaluation results.

4. Computer Vision and Its Role in Intrusion Detection

Computer vision plays a critical role in immediate intrusion detection systems. It enables machines to interpret and make decisions based on visual data, much like human vision. The detection of individuals and new faces, a fundamental aspect of intrusion detection, relies heavily on advanced algorithms in image processing technology. Prior research has explored several methodologies for face detection and recognition, ranging from traditional image processing techniques to deep learning-based models. Convolutional Neural Networks (CNNs) have proven particularly effective in recognizing faces, as they can automatically learn hierarchical representations of visual data. Studies such as Zhang et al. (2020) have shown that CNN-based models outperform earlier face detection algorithms, reducing false-positive rates and increasing accuracy in real-world environments where lighting conditions, angles, and occlusions vary.

5. Machine Learning for Analyzing Sentiment and Behavior

Beyond face recognition, ML techniques techniques are pivotal for analyzing sentiment and behavior in immediate intrusion detection systems. Sentiment analysis, which involves determining the emotional state of individuals, can aid in detecting potential threats based on expressions or body language. Research by Sharma et al. (2019) emphasizes the application of recurrent neural networks (RNNs) and Long Short- Term Memory (LSTM) networks in processing video frames to analyze human emotions in real time. Such models can classify behaviors into various categories—such as calm, agitated, or threatening—enabling the system to alert security personnel before incidents escalate.

However, one major challenge in using ML for sentiment analysis in monitoring is the variability in human expressions and cultural differences in interpreting emotions. Existing models must be trained on diverse datasets to handle a wide range of individuals, environments, and behavioral cues. Another issue lies in the computational intensity of immediate processing, which requires highly optimized algorithms to avoid latency in threat detection.

6. Artificial intelligence and Weapon Detection in Real-Time Security

One of the most critical features of immediate intrusion detection systems is the identification of potential physical threats, particularly weapons. artificial intelligence models have been developed to recognize guns, knives, and other dangerous objects by analyzing visual data. Deep learning techniques, especially object detection algorithms like YOLO (You Only Look Once) and Faster R-CNN, have been widely adopted for this purpose. According to Nguyen et al. (2021), YOLO offers an efficient and immediate solution for detecting weapons in crowded and complex environments, owing to its ability to process images quickly and accurately without requiring high computational resources.

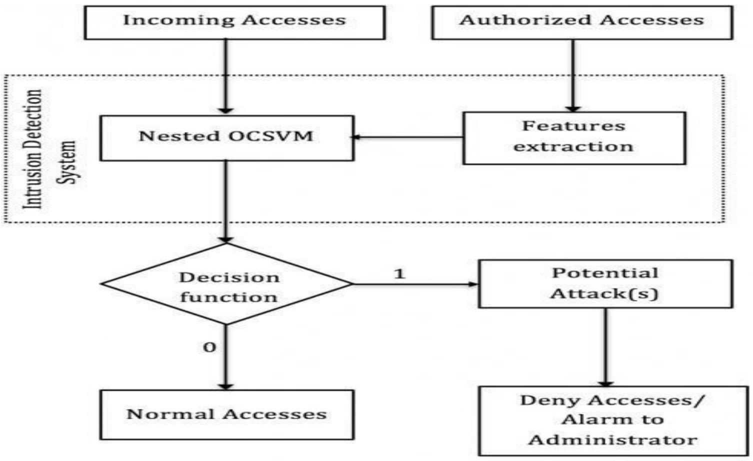

Figure 2 Proposed Workflow

However, weapon detection in real-world settings is not without challenges. Factors such as occlusion (where a weapon might be partially concealed), variations in lighting, and the rapid movement of individuals can affect the system's accuracy. Several studies recommend augmenting artificial intelligence weapon detection systems with multi-modal sensors, such as thermal imaging and infrared sensors, to improve detection rates in poor visibility conditions.

7. Real-Time Surveillance and User Updates with Approval Mechanisms

One of the most unique features of the "Real-Time Intrusion Detection System" is ability to update users with photographs of suspicious individuals. This enhances situational awareness and enables immediate response actions. In addition to providing immediate alerts, the system offers an approval mechanism for known individuals. If the system detects a suspicious person but the user recognizes the individual as a relative or acquaintance, the user can grant access directly through the alert interface. This feature provides a level of flexibility, ensuring that security systems are not overly restrictive, while still maintaining high standards of safety.

This approval mechanism can be highly beneficial in residential and corporate settings, where the system must distinguish between actual threats and benign situations involving familiar faces. Research into this area, as discussed by Khan et al. (2022), highlights the importance of user-friendly interfaces and secure communication channels that allow for quick decision-making. However, to ensure security, the system must also have built-in safeguards to prevent unauthorized access, such as multi-factor authentication or a time- limited response window.

8. Challenges and Limitations

While immediate intrusion detection systems using image processing technology, ML, and artificial intelligence have shown remarkable potential, several challenges remain. First, the accuracy of detection systems is highly dependent on the quality and size of the dataset used for training artificial intelligence models. In many cases, existing datasets are not representative of the vast range of real-world scenarios, leading to performance issues when systems are deployed in dynamic environments. Second, the immediate nature of these systems requires significant computational resources, and the trade-off between processing speed and accuracy must be carefully balanced. Hardware acceleration techniques, such as the use of GPUs and edge computing, have been suggested as possible solutions to mitigate these challenges.

Moreover, ethical concerns regarding monitoring technologies cannot be overlooked. The constant monitoring of individuals raises questions about the right to privacy and the potential for abuse in the hands of governments or corporations. Future research must address these ethical considerations and ensure that immediate intrusion detection systems are deployed responsibly, with appropriate checks and balances in place.

9. Conclusion and Future Directions

The research on immediate intrusion detection systems using image processing technology, ML techniques, and artificial intelligence reflects significant progress in the field of monitoring and security. These systems can enhance safety by detecting suspicious behavior, recognizing weapons, and providing immediate updates to users. However, challenges such as dataset limitations, computational demands, and ethical concerns must be addressed to fully realize the potential of these technologies.

Future research should focus on improving the robustness of artificial intelligence models to handle diverse real-world scenarios, integrating multi-modal sensors for enhanced accuracy, and developing legal frameworks to govern the use of such systems in public spaces. Additionally, the rise of edge computing and 5G networks may offer new opportunities to overcome the computational constraints associated with immediate processing, enabling even faster and more accurate intrusion detection systems.

References

1. Agustina J. R. and Clavell G (2019) "The Impact of CCTV on Fundamental Rights and Crime Prevention Strategies: The Case of the Catalan Control Commission of Video Surveillance Devices," Computer Law and Security Review, pp. 168-174, doi:10.1016/j.clsr.2020.01.006.
2. Banuchitra S and Kungumaraj K (2019) "A comprehensive survey of content-based image retrieval techniques," International Journal of Engineering and Computer Science, vol.5, no.8, pp.17577-17584, doi:10.18535/ijecs/v5i8.26.
3. Çarıkçı M and Özen F (2021) "A face recognition system based on eigenfaces method," Procedia Technology, vol. 1, doi:10.1016/j.protcy.2012.02.023 pp. 118-123.
4. Chang X , Nie F ,Wang S ,Yang Y, Zhou X, and C. Zhang (2019) "Compound rank-k projections for bilinear analysis," IEEE Transactions on Neural Networks and Learning Systems, vol. 27, no. 7, pp. 1502–1513. IJISAE, 2024, 12(5s), 295–300 | 299 International Journal of Intelligent Systems and Applications in Engineering.
5. Elfasakhany, Hernández J, García J. C, Reyes M, Martell F (2020) "Design and development of a house- mobile security system," Engineering, vol.03,no.12,pp.1213 1224,doi:10.4236/eng.2011.312151.
6. Faux Fand Luthon F (2019) "Theory of evidence for face detection and tracking," International Journal of Approximate Reasoning, vol. 53, no. 5, pp. 728 746,doi:10.1016/j.ijar.2019.02.002.
7. Li S (2020) "The application of face recognition based on opencv," Advanced Materials Research, vol.403- 408, pp.2350.
8. Li W ,Zhao R ,Xiao T, and Wang X (2019) "Deepreid: Deep filter pairing neural network for person re- identification," in Proc. CVPR, pp. 152 159. Liao S, Hu Y, Zhu X, and Li S Z (2018) "Person re identification by local maximal occurrence representation and metric learning," in Proc. CVPR, pp. 2197– 2206.
9. Ni Jand Chellappa R (2022), "Evaluation of state-of the-art algorithms for remote face recognition," IEEE International Conference on Processing,doi:10.1109/icip.2010.5652608.
10. Reza Khan S and Sultana Dristy F (2020) "Android based security and Home Automation System", "The International Journal of Ambient Systems and Applications", vol. 3, no. 1, pp. 15-24, doi: 10.5121/ijasa.2014.3102.

AUTHORS

Bindu Rani has received M.tech degree in Computer Science and Engineering. She is currently working as an Assistant Professor in Computer Science and Engineering (AIML) department at MIT with 9 year of professional experience. She has wide expertise in Artificial Intelligence & Machine Learning.

Vinay Kumar Pant has received M.tech degree in Computer Science and Engineering. He is currently working as an Assistant Professor in Computer Science and Engineering (AIML) department at MIT with 9 year of professional experience. He has wide expertise in Artificial Intelligence & Machine Learning.

Naman Sharma is a B.Tech 4th year student in computer science and engineering(specialization in artificial intelligence and machine learning) department at Moradabad Institute of Technology affiliated with Dr APJ Abdul Kalam Technical University his research interest including Machine Learning, Artificial Intelligence and Natural Processing Language, Python and SQL.

Mohd. Mudassir is a B.Tech 4th year student in computer science and engineering(Specialization in artificial intelligence and machine learning) department at Moradabad Institute of Technology affiliated with Dr APJ Abdul Kalam Technical University his research interest including Machine Learning, Artificial Intelligence , Python and SQL.

Arzan Hussain is a B.Tech 4th year student in computer science and engineering(specialization in artificial intelligence and machine learning) department at Moradabad Institute of Technology affiliated with Dr APJ Abdul Kalam Technical University his research interest include ML,AI and python.

a B.Tech 4th year student in computer science and engineering(specialization in artificial intelligence and machine learning) department at Moradabad Institute of Technology affiliated with Dr APJ Abdul Kalam Technical University his research interest include ML and python.