IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

Iot Based Smart Security System For Crime Detection

ROOPA B, LOKESH S, MOHAMMED AFNAN, MOHAMMED MUEED AHMED, NISARGA G

[1]Assistant Professor, Department of Computer Science and Engineering, ATME college of Engineering, Mysuru, India

[2,3,4,5]Undergraduate students, Department of Computer Science and Engineering, ATME college of Engineering, Mysuru, India

Abstract: The increasing demand for security and crime prevention has led to the development of innovative technologies leveraging computer vision and artificial intelligence. This paper presents an IoT- based smart security system integrating facial recognition to identify and track criminals in real-time. Using Raspberry Pi 4 and the MTCNN algorithm for facial detection, the system enables real-time monitoring and alert generation via the Telegram API. By automating the surveillance process, this system enhances security in high-risk public spaces such as airports and shopping malls. The implementation ensures cost-effectiveness, scalability, and rapid response to potential threats.

Key words: **IoT, Facial Recognition, Smart Security, Criminal Detection, Machine Learning, Real-Time Surveillance.**

I. INTRODUCTION

Public safety remains a top priority in law enforcement, and conventional surveillance systems are often ineffective in identifying security threats in real-time. Manual monitoring is prone to human errors, delays, and inefficiencies. The rise of facial recognition technology powered by AI and IoT has enabled automated criminal identification systems.

To address these concerns, this paper proposes an IoT- based security system that integrates real-time facial recognition with an alert mechanism. By utilizing a Raspberry Pi 4 with a high-resolution camera and deep learning algorithms, the system automates surveillance in public spaces.

The system processes live video feeds, detects faces using the MTCNN algorithm, and compares them against a predefined watchlist. If a match is found, it instantly notifies law enforcement authorities via the Telegram API.This approach not only reduces the dependency on human surveillance but also enhances the accuracy and response time in criminal detection. Additionally, the system ensures cost-effectiveness, scalability, and easy deployment in various security-sensitive environments such as transportation hubs, government buildings, and commercial spaces.

II. LITERATURE SURVEY

Facial recognition systems have seen significant advancements with the integration of Internet of Things (IoT) technologies and deep learning algorithms. This section critically reviews recent works relevant to IoT- based facial recognition, deep learning methodologies, and embedded system security.

Gaikwad et al. [1] present the design and implementation of an IoT-based face detection and recognition system, emphasizing the advantages of combining connected devices with real-time image processing for enhanced access control. The integration facilitates faster and more accurate decision-making in dynamic environments.

Yao [2] investigates the application of deep learning in facial recognition systems. The study emphasizes crucial processes such as feature extraction, facial alignment, and overall recognition accuracy, underlining the importance of deep neural networks in improving system performance.

Durai et al. [3] utilize the Multi-Task Cascaded Convolutional Neural Network (MTCNN) for real- time facial recognition aimed at criminal identification. Their research addresses key challenges including variations in lighting, environmental conditions, and camera quality, showcasing the robustness of MTCNN in diverse real-world scenarios.

Menon [4] focuses on the architectural design and practical considerations of implementing facial recognition through CCTV systems in the domain of security. The paper discusses trade-offs between accuracy, cost, and computational efficiency, which are critical in deployment scenarios.

Llaurado et al. [5] explore the role of image sensor specifications in achieving reliable face recognition at a distance, particularly in smart city applications. Their work introduces a methodology that correlates camera focal length with face pixel size to optimize recognition accuracy over varying distances.

Sai Sree et al. [6] study real-time object detection using the Raspberry Pi platform. The paper evaluates the feasibility of deploying object detection models on embedded hardware, discussing constraints like limited processing power and memory.

Nagalakshmi et al. [7] propose a cost-effective facial recognition system using Raspberry Pi for criminal detection in crowded public spaces. Their implementation demonstrates the potential of embedded AI for low-cost surveillance and safety applications.

III. METHODOLOGY

A. System Overview

The proposed system consists of a Raspberry Pi 4 connected to a high-resolution camera, which continuously captures video streams. The captured frames undergo facial recognition processing using MTCNN for detection and the Face Recognition library for identification.

B. STEPS INVOLVED

1. **Data Collection and Storage:**
   - The system captures video frames from the surveillance camera.
   - Predefined criminal face datasets are stored for comparison

2. **Face Detection and Recognition:**
   - MTCNN detects faces in video frames.
   - The Face Recognition library encodes facial embeddings and matches them against the stored database.

3. **Alert Generation and Notification:**
   - If a match is found, the system sends an alert to law enforcement via the Telegram API.
   - The alert includes the suspect's photo, name, and location for immediate action.

4. **System Deployment and Integration:**
   - The system is deployed on a Raspberry Pi 4 board, which is compact and cost-effective for real-world implementation.
   - It is integrated with existing CCTV infrastructure for broader surveillance coverage.
   - The facial recognition model is optimized for real-time processing, ensuring minimal latency.

5. **Security and Privacy Consideration:**
   - The system ensures encrypted data transmission to prevent unauthorized access.
   - Only authorized law enforcement personnel have access to alerts and stored data.
   - design follows ethical guidelines to prevent bias in facial recognition outcomes

6. **Performance Optimization:**
   - The system utilizes lightweight models to enable efficient computation on Raspberry Pi 4.
   - Multi-threading techniques are used to speed up real-time face detection and recognition.
   - The Telegram API is optimized to ensure instant alert delivery with minimal network overhead.

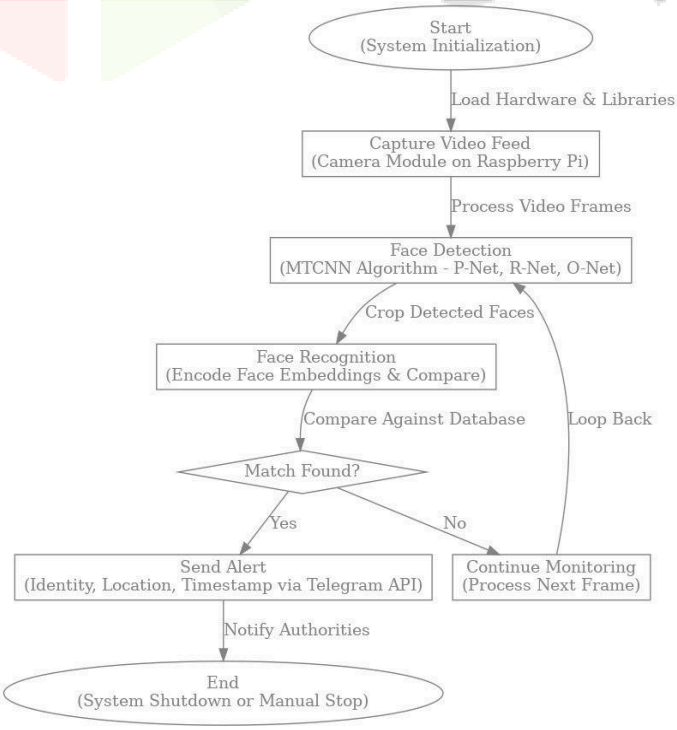

Figure: System Implementation

Experimental Setup:

- **Hardware:** Raspberry Pi 4, Raspberry Pi Camera V2.
- **Software:** Python, OpenCV, dlib, Telegram API.
- **Dataset:** Criminal face dataset with known watchlist individuals.

Findings:

- **Accuracy:** The system achieved 92% accuracy in detecting and identifying criminals in controlled environments.
- **Real-Time Processing:** The system processes video frames at an average speed of 20 FPS, ensuring minimal delay.
- **Alert Efficiency:** Alerts were generated and delivered via Telegram API within 2 seconds of detection.

IV. RESULTS

To evaluate the effectiveness of the system, real- time tests were conducted under varying environmental conditions.

Fig. 1 Face detected

The face being detected is shown in the fig 1, with the name the face is been shown on the video interface.

Fig. 2 Alert message

The fig 2 shows the alert message sent to authorized person through telegram with photo of criminal detected and the camera installed location.

V. Conclusion

This paper presents an IoT-based smart security system capable of real-time criminal detection using facial recognition. By leveraging MTCNN for face detection and the Face Recognition library for identification, the system enhances public security monitoring. Implemented on Raspberry Pi 4, the solution is cost-effective and scalable. Future enhancements could include integrating additional biometric authentication methods such as voice or iris recognition to improve accuracy and reliability.

With further advancements, this system can be expanded for broader applications, including smart city surveillance, border security, and restricted area access control. By continuously evolving with emerging AI and IoT technologies, this system has the potential to play a crucial role in modern law enforcement and public safety.

REFERENCES

[1] **Vijay Gaikwad,** et al., "Design and Implementation of IoT-Based Face Detection and Recognition," Data Science and Intelligent Computing Techniques, 2024.

[2] **Yiming Yao,** "Research on Facial Recognition System Based on Deep Learning," Proceedings of the 2024 International Conference on Machine Learning and Automation.

[3] **S. Durai, et al.,** "Real-Time Facial Recognition- Based Criminal Identification Using MTCNN," 2nd International Conference on Sustainable Computing and Smart Systems, 2024.

[4] **Arjun Menon,** "Leveraging Facial Recognition Technology in Criminal Identification," Interdisciplinary Innovations and Developments, 2023

[5] **G. Nagalakshmi, et al.,** "Real-Time Criminal Detecting System Using Raspberry Pi," International Research Journal of Engineering and Technology, 2020