A Project Report

On

**AI GUN**

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY, PUNE

IN PARTIAL FULFILLMENT OF THE REQUIREMENTS

FOR THE PROJECT-BASED LEARNING II

By

**32 – Kashyap Kamble**

**37 – Aadesh Lawande**

**57 – Stavan Shere**

Under the guidance

of

**PROF. GAJANAN BHUSARE**



**DEPARTMENT OF ARTIFICIAL INTELLIGENCE AND DATA SCIENCE ENGINEERING**

**Zeal Educational Institute’s**

**Zeal College of Engineering and Research, Pune**

Accredited with ‘A+’ grade by NAAC

**Savitribai Phule Pune University**

**2023-24**

****

**Zeal Education Society’s**

**ZEAL COLLEGE OF ENGINEERING & RESEARCH, Pune**

**Accredited with ‘A+’ grade by NAAC**

**CERTIFICATE**

­

This is to certify that the PBL IIreport entitled

**“AI GUN”**

Submitted by

**Mr. Kashyap Kamble Exam Seat No: S190532044**

**Mr. Aadesh Lawande Exam Seat No: S190532054**

**Mr. Stavan Shere Exam Seat No: S190532084**

of S.E. AI & DS Engineering has satisfactorily delivered his/her project and it is submitted towards the partial fulfillment of the requirement of Savitribai Phule Pune University, under the Department of AI & DS, ZCOER, Pune for the PROJECT BASED LEARNING II.

**Prof.Gajanan Bhusare** **Prof. Dikshendra Sarpate**

Internal Guide Head

Department of AI & DS Department of AI & DS

Internal Examiner: (Name) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Sign) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

External Examiner: (Name) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (Sign) \_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Seal/Stamp of the College

Place: **PRINCIPAL**

Date:

**CERTIFICATE BY GUIDE**

This is to certify that **Kashyap Kamble** has completed the dissertation work under my guidance and supervision and that, I have verified the work for its originality in documentation, problem statement, implementation and result presented in the dissertation. Any reproduction of the other necessary work is with the prior permission and has given due ownership and included in the references.

Signature of Guide

(Prof. **Gajanan Bhusare**)

**CERTIFICATE BY GUIDE**

This is to certify that **Aadesh lawande** has completed the dissertation work under my guidance and supervision and that, I have verified the work for its originality in documentation, problem statement, implementation and result presented in the dissertation. Any reproduction of the other necessary work is with the prior permission and has given due ownership and included in the references.

Signature of Guide

(Prof. **Gajanan Bhusare**)

**CERTIFICATE BY GUIDE**

This is to certify that **Stavan Shere** has completed the dissertation work under my guidance and supervision and that, I have verified the work for its originality in documentation, problem statement, implementation and result presented in the dissertation. Any reproduction of the other necessary work is with the prior permission and has given due ownership and included in the references.

Signature of Guide

(Prof. **Gajanan Bhusare**)

**ACKNOWLEDGEMENT**

I take this opportunity to express my deep sense of gratitude towards my esteemed guide **Prof. Gajanan Bhusare** for giving me this splendid opportunity to select and present this dissertation and also providing facilities for successful completion.

I thank **Dikshendra Sarpate**, Head, Department of Artificial Intelligence and Data Science Engineering, for opening the doors of the department towards the realization of the seminar, all the staff members, for their indispensable support, priceless suggestions and for most valuable time lent as and when required. With all the respect and gratitude, I would like to thank all the people, who have helped me directly or indirectly.

**Name of Students: Kashyap Kamble ,Aadesh Lawande , Stavan Shere**

Class Roll No. : S1411032 , S14111037 , S1411057

Exam Seat No: S190532044 , S190532054 , S190532084

**ABSTRACT**

**AI GUN is a system designed to enhance security measures by integrating artificial intelligence (AI) with surveillance systems. Traditional surveillance systems often rely on human operators to monitor video feeds, which can be time-consuming and prone to errors. AI GUN automates this process by using computer vision and machine learning algorithms to detect and recognize potential threats in real-time video streams.**

**The core functionality of AI GUN includes:**

1. **Object Detection and Recognition: AI GUN employs state-of-the-art object detection algorithms to identify various objects, such as people, vehicles, and weapons, in the video feed. Deep learning models are trained on large datasets to achieve high accuracy in recognizing these objects.**
2. **Threat Assessment: Once objects are detected, AI GUN assesses the threat level associated with each detected object based on predefined criteria. For example, it can analyze the behavior of individuals or the presence of weapons to determine potential threats to security.**
3. **Alert Generation: In the event of a potential threat, AI GUN generates real-time alerts to notify security personnel or authorities. These alerts can include detailed information about the detected threat, such as the location, timestamp, and type of object detected.**
4. **Integration with Existing Systems: AI GUN is designed to seamlessly integrate with existing surveillance infrastructure, including CCTV cameras, drones, and other sensors. It can also be integrated with centralized monitoring systems and security management platforms to streamline security operations.**
5. **Continuous Learning and Adaptation: AI GUN continuously learns from new data and feedback to improve its detection capabilities over time. It adapts to changing environments and evolving threat landscapes to maintain high performance and reliability.**

**AI GUN offers several advantages over traditional surveillance methods, including improved accuracy, faster response times, and reduced reliance on human operators. By leveraging the power of AI, AI GUN enhances security measures and helps organizations better protect their assets, infrastructure, and personnel from potential threats**

**CONTENTS**

1. **Introduction.**
2. **Key Components**
3. **Methodology Used**
4. **Challenges**
5. **Applications**
6. **Technological Advancements**
7. **Future Directions**
8. **Code and output**
9. **Conclusion**

**INTRODUCTION:**

**AI GUN represents a groundbreaking advancement in security technology, revolutionizing the way surveillance systems operate to ensure public safety and protect critical infrastructure. In today's rapidly evolving security landscape, the need for proactive threat detection and rapid response capabilities has never been greater. Traditional surveillance methods, reliant on human operators and manual monitoring, are often inadequate in effectively addressing emerging security threats.**

**AI GUN addresses these challenges by harnessing the power of artificial intelligence (AI) to analyze vast amounts of video data in real-time. By leveraging computer vision algorithms and machine learning models, AI GUN can automatically detect and recognize various objects, including people, vehicles, and weapons, within video streams. This enables security personnel to swiftly identify potential threats and take appropriate action to mitigate risks.**

**Key features of AI GUN include its ability to assess the threat level associated with detected objects, generate real-time alerts to notify security personnel, and seamlessly integrate with existing surveillance infrastructure. Furthermore, AI GUN continuously learns from new data and feedback to improve its detection capabilities over time, ensuring adaptability to evolving security challenges.**

**In this report, we delve into the core components, methodologies, challenges, applications, technological advancements, future directions, and conclusions surrounding AI GUN. By exploring these aspects, we aim to provide a comprehensive understanding of how AI GUN is reshaping the landscape of security technology and enhancing public safety on a global scale.**

**Top of Form**

**KEY COMPONENTS OF AI GUN:**

1. **Object Detection and Recognition Algorithms: Object detection and recognition algorithms form the backbone of AI GUN. These algorithms utilize computer vision techniques to analyze video streams and identify various objects of interest, including people, vehicles, and weapons. State-of-the-art deep learning models, such as convolutional neural networks (CNNs), are commonly employed to achieve high accuracy in detecting and recognizing objects in real time.**
2. **Threat Assessment Mechanisms: AI GUN incorporates sophisticated threat assessment mechanisms to evaluate the risk level associated with detected objects. These mechanisms analyze contextual information, such as object behavior, location, and environmental factors, to determine the likelihood of a threat. By assessing the severity of potential threats, AI GUN enables security personnel to prioritize responses and allocate resources effectively.**
3. **Alert Generation Systems: Upon detecting a potential threat, AI GUN generates real-time alerts to notify security personnel or authorities. These alerts include detailed information about the detected object, such as its type, location, and timestamp. Alerts can be delivered through various communication channels, including mobile devices, email, and centralized monitoring systems, ensuring timely response to security incidents.**
4. **Integration with Existing Surveillance Infrastructure: AI GUN is designed to seamlessly integrate with existing surveillance infrastructure, including closed-circuit television (CCTV) cameras, drones, and sensors. It can interface with video management systems (VMS), security information and event management (SIEM) platforms, and other security solutions to enhance overall situational awareness and response capabilities.**
5. **Continuous Learning and Adaptation: AI GUN employs machine learning techniques to continuously learn from new data and feedback. By analyzing historical data and user interactions, AI GUN improves its detection capabilities over time and adapts to changing security threats and environments. This iterative learning process ensures that AI GUN remains effective and reliable in detecting emerging threats and minimizing false alarms.**

**These key components collectively enable AI GUN to enhance security measures by automating threat detection, facilitating rapid response, and providing actionable intelligence to security personnel. By leveraging advanced technologies such as artificial intelligence and computer vision, AI GUN represents a significant advancement in the field of security technology.**

**METHODOLOGY USED:**

**The development and implementation of AI GUN involve a comprehensive methodology that encompasses several stages, including data collection, preprocessing, algorithm selection, model training, evaluation, and deployment. The following outlines the methodology used in the creation of AI GUN:**

1. **Data Collection: The first step in developing AI GUN involves collecting a diverse and representative dataset of video feeds from surveillance cameras or other sources. This dataset should include examples of various objects of interest, such as people, vehicles, and weapons, in different environments and lighting conditions.**
2. **Data Preprocessing: Once the dataset is collected, it undergoes preprocessing to prepare it for training. This may involve tasks such as resizing images, normalizing pixel values, and augmenting the dataset with variations to improve model generalization.**
3. **Algorithm Selection: Next, suitable algorithms for object detection, recognition, and threat assessment are selected based on the specific requirements and constraints of the application. State-of-the-art deep learning models, such as convolutional neural networks (CNNs) and recurrent neural networks (RNNs), are commonly used for these tasks due to their effectiveness in processing visual data.**
4. **Model Training: The selected algorithms are trained on the preprocessed dataset to learn patterns and features associated with different objects and threat scenarios. During training, the model optimizes its parameters to minimize a specified loss function, typically using techniques such as backpropagation and gradient descent.**
5. **Evaluation: After training, the performance of the AI GUN model is evaluated using separate validation and test datasets. Metrics such as precision, recall, and F1 score are calculated to assess the model's accuracy, robustness, and generalization capabilities. The model may undergo iterative refinement based on evaluation results to improve performance.**
6. **Deployment: Once the AI GUN model meets the desired performance criteria, it is deployed in production environments for real-time operation. This involves integrating the model with existing surveillance infrastructure, setting up monitoring systems, and configuring alert generation mechanisms. Continuous monitoring and maintenance are essential to ensure optimal performance and reliability over time.**
7. **Continuous Learning: AI GUN incorporates mechanisms for continuous learning and adaptation to evolving security threats and environments. This involves periodically retraining the model with new data, updating algorithms and parameters, and integrating feedback from security personnel and system users.**

**By following this methodology, AI GUN can effectively detect and mitigate security threats in real-time, providing enhanced safety and security in various applications and environments.**

**Top of Form**

**Bottom of Form**

**CHALLENGES IN AI GUN:**

1. **Algorithm Accuracy: One of the primary challenges in AI GUN is achieving high accuracy in object detection and threat assessment. Variations in lighting conditions, occlusions, and object appearances can lead to false positives or missed detections, compromising the reliability of the system.**
2. **Real-Time Processing Requirements: AI GUN must process video feeds in real-time to enable timely threat detection and response. Meeting the computational demands of real-time processing while maintaining high accuracy poses a significant technical challenge, particularly in resource-constrained environments.**
3. **Data Privacy Concerns: The use of AI GUN raises privacy concerns related to the collection and analysis of video data. Ensuring compliance with data protection regulations and safeguarding sensitive information from unauthorized access or misuse is essential to maintain public trust and legal compliance.**
4. **Ethical Considerations: AI GUN may encounter ethical dilemmas related to bias, fairness, and accountability in decision-making. Biased algorithms or inaccurate assessments could lead to discriminatory outcomes or unjustified actions, highlighting the importance of ethical oversight and responsible AI development.**
5. **Integration Complexity: Integrating AI GUN with existing surveillance infrastructure and security systems can be complex and time-consuming. Compatibility issues, interoperability challenges, and customization requirements may arise, necessitating careful planning and coordination with stakeholders.**
6. **Adversarial Attacks: AI GUN is vulnerable to adversarial attacks, where malicious actors manipulate inputs to deceive or evade detection. Robustness against adversarial attacks is crucial to ensure the reliability and effectiveness of the system in real-world scenarios.**
7. **Scalability: AI GUN must be scalable to accommodate growing data volumes, increasing computational demands, and evolving security requirements. Scalability challenges include optimizing resource utilization, minimizing latency, and supporting distributed deployments across multiple locations.**
8. **Human-Machine Interaction: Effective collaboration between AI GUN and human operators is essential for interpreting alerts, making informed decisions, and responding to security incidents. Designing intuitive user interfaces, providing actionable intelligence, and facilitating seamless communication are key challenges in human-machine interaction.**

**Addressing these challenges requires a multidisciplinary approach involving expertise in artificial intelligence, computer vision, cybersecurity, privacy, ethics, and human factors. By overcoming these challenges, AI GUN can realize its potential to enhance security measures and improve public safety in diverse environments and applications.**

**APPLICATIONS OF AI GUN:**

**1. Public Safety and Law Enforcement:**

**AI GUN can be deployed in public spaces, transportation hubs, and urban areas to enhance public safety and support law enforcement efforts. It enables real-time monitoring of crowds, identification of suspicious behavior, and detection of unauthorized objects or activities, helping to prevent crimes and respond to security incidents effectively.**

**2. Critical Infrastructure Protection:**

**AI GUN is used to safeguard critical infrastructure, such as power plants, airports, and government facilities, from security threats and potential terrorist attacks. It continuously monitors perimeter areas, identifies intrusions or security breaches, and alerts security personnel to take appropriate action to mitigate risks and ensure the integrity of critical assets.**

**3. Border Security and Immigration Control:**

**AI GUN plays a vital role in border security and immigration control by monitoring border crossings, ports of entry, and immigration checkpoints. It detects unauthorized border crossings, identifies individuals on watchlists or with fraudulent documents, and assists border patrol agents in intercepting illegal immigrants, smugglers, and traffickers.**

**4. Counterterrorism and Counterinsurgency:**

**AI GUN supports counterterrorism and counterinsurgency operations by detecting and neutralizing threats posed by terrorist organizations, extremist groups, and insurgent movements. It identifies suspicious individuals, vehicles, and objects in high-risk areas, facilitates preemptive strikes against terrorist cells, and disrupts terrorist activities before they can be carried out.**

**5. Event Security and Crowd Management:**

**AI GUN is utilized in event security and crowd management to ensure the safety of attendees and prevent security incidents during large gatherings, such as concerts, sporting events, and political rallies. It monitors crowd movements, identifies potential security risks, and coordinates emergency responses to maintain order and minimize disruptions.**

**6. Transportation Security:**

**AI GUN is deployed in transportation systems, including airports, seaports, and railway stations, to enhance security screening and threat detection measures. It scans luggage, cargo, and passengers for prohibited items, detects suspicious behavior or anomalies, and helps authorities intercept threats before they can board or enter transportation vehicles.**

**7. Private Sector Security:**

**AI GUN is adopted by private sector organizations, such as corporations, banks, and retail establishments, to protect their assets, employees, and customers from security threats and criminal activities. It monitors premises, identifies potential security breaches, and assists security teams in responding to incidents in real-time, ensuring the safety and security of personnel and assets.**

**These applications demonstrate the diverse range of use cases for AI GUN in enhancing security measures and protecting individuals, infrastructure, and assets from various threats and security risks. By leveraging advanced technologies such as artificial intelligence and computer vision, AI GUN contributes to improving overall security and public safety in both public and private settings.**

**TECHNOLOGICAL ADVANCEMENTS:**

**1. Advanced Object Detection Algorithms:**

**Technological advancements in object detection algorithms, particularly in the field of deep learning, have significantly improved the accuracy and efficiency of AI GUN systems. State-of-the-art convolutional neural networks (CNNs) and other deep learning architectures can accurately detect and recognize objects of interest, including people, vehicles, and weapons, in complex and dynamic environments.**

**2. Real-Time Processing Capabilities:**

**Advancements in hardware acceleration technologies, such as graphics processing units (GPUs) and tensor processing units (TPUs), have enabled AI GUN systems to perform real-time processing of high-resolution video streams with minimal latency. This allows for timely threat detection and rapid response capabilities, enhancing overall security effectiveness.**

**3. Edge Computing and IoT Integration:**

**Integration of AI GUN with edge computing platforms and Internet of Things (IoT) devices enables distributed processing and decentralized decision-making at the network edge. Edge-based AI GUN systems can analyze video feeds locally, reducing bandwidth requirements and improving responsiveness, making them well-suited for applications in remote or bandwidth-constrained environments.**

**4. Multi-Sensor Fusion:**

**Technological advancements in sensor technologies, such as LiDAR, radar, and thermal imaging, enable AI GUN systems to leverage multi-sensor fusion techniques for enhanced situational awareness. By combining data from multiple sensors, AI GUN can provide comprehensive coverage, detect threats across different modalities, and improve detection accuracy in challenging conditions, such as low visibility or adverse weather.**

**5. Explainable AI and Interpretability:**

**Developments in explainable AI (XAI) techniques enable AI GUN systems to provide transparent and interpretable explanations for their decisions and predictions. By understanding the underlying rationale behind AI GUN's outputs, security personnel can better trust and validate the system's recommendations, enhancing confidence in its effectiveness and reliability.**

**6. Autonomous Surveillance Drones:**

**Integration of AI GUN with autonomous surveillance drones enables aerial monitoring of large areas and inaccessible terrain, such as border regions, coastlines, and critical infrastructure sites. AI-powered drones equipped with advanced sensors and onboard processing capabilities can autonomously detect and track potential threats, providing aerial surveillance and reconnaissance capabilities to enhance security operations.**

**7. Cloud-Based Analytics and Collaboration:**

**Cloud-based analytics platforms and collaboration tools facilitate centralized data storage, analysis, and collaboration among multiple stakeholders in AI GUN deployments. Cloud-enabled AI GUN systems can leverage scalable computing resources, share real-time intelligence across distributed teams, and support collaborative decision-making processes, enhancing overall security coordination and effectiveness.**

**These technological advancements collectively contribute to the continued evolution and enhancement of AI GUN systems, enabling them to address emerging security challenges and meet the evolving needs of users in diverse applications and environments.**

**FUTURE DIRECTIONS:**

**1. Enhanced Autonomous Capabilities:**

**Future advancements in AI GUN will focus on enhancing autonomous capabilities, enabling systems to operate with minimal human intervention. This includes the development of self-learning algorithms, adaptive decision-making mechanisms, and autonomous response capabilities to handle complex security scenarios and dynamic environments effectively.**

**2. Multi-Modal Sensing and Fusion:**

**The integration of multi-modal sensing technologies, such as vision, audio, and environmental sensors, will enable AI GUN systems to gather richer and more comprehensive data for threat detection and assessment. Future systems will leverage advanced sensor fusion techniques to integrate data from diverse sources and improve situational awareness in complex and challenging environments.**

**3. Predictive Analytics and Preemptive Threat Detection:**

**AI GUN systems will evolve to incorporate predictive analytics capabilities, enabling them to anticipate and preempt security threats before they occur. By analyzing historical data, identifying patterns, and predicting potential threats, future systems can proactively deploy resources, implement preventive measures, and mitigate risks to enhance overall security preparedness and resilience.**

**4. Human-Centric Design and Explainable AI:**

**Future AI GUN systems will prioritize human-centric design principles and incorporate explainable AI (XAI) techniques to enhance transparency, trust, and usability. Systems will provide interpretable explanations for their decisions, facilitate user interaction and feedback, and empower security personnel to understand, validate, and effectively utilize AI-generated insights and recommendations.**

**5. Edge Intelligence and Decentralized Processing:**

**Advancements in edge computing and decentralized processing technologies will enable AI GUN systems to operate autonomously and efficiently at the network edge. Edge-enabled systems will perform real-time processing, minimize latency, and conserve bandwidth by analyzing data locally, making them well-suited for deployment in remote or resource-constrained environments.**

**6. Robustness and Resilience Against Adversarial Attacks:**

**Future AI GUN systems will incorporate robustness and resilience mechanisms to defend against adversarial attacks and manipulation attempts. This includes the development of robust algorithms, adversarial training techniques, and anomaly detection mechanisms to detect and mitigate threats posed by malicious actors seeking to deceive or evade detection.**

**7. Collaborative and Interoperable Security Ecosystems:**

**Future AI GUN deployments will prioritize collaboration and interoperability among diverse security systems and stakeholders. Integrated security ecosystems will facilitate data sharing, coordination, and collaboration across organizational boundaries, enabling seamless information exchange, joint threat analysis, and coordinated response efforts to address complex security challenges effectively.**

**By focusing on these future directions, AI GUN systems will continue to evolve and advance, enabling organizations and authorities to enhance security measures, protect critical assets, and ensure public safety in an increasingly complex and dynamic security landscape.**

CODE:

# Importing the libraries

from PIL import Image

import cv2

import numpy as np

import pyfirmata

from keras.models import load\_model

board = pyfirmata.Arduino('COM5')

pan\_pin = board.get\_pin('d:9:s') # Digital pin 9 for pan servo

tilt\_pin = board.get\_pin('d:10:s')

def mirror\_value(val,):

midpoint = (0 + 180) / 2

mirror\_val = midpoint - (val - midpoint)

return mirror\_val

def make\_positive(n):

if n < 0:

return -n # Return the absolute value

return n

def map\_value(value, from\_min, from\_max, to\_min, to\_max):

return int((value - from\_min) \* (to\_max - to\_min) / (from\_max - from\_min) + to\_min)

# Load the pretrained model

model = load\_model('C:/Users/Aadesh/A.i\_gun/Face-mask-detection/maskDetectionModel.h5')

# Loading the cascades to detect human faces

face\_cascade = cv2.CascadeClassifier('C:/Users/Aadesh/A.i\_gun/Face-mask-detection/haarcascade\_frontalface\_default.xml')

def face\_extractor(img):

# Function detects faces and returns the cropped face

# If no face detected, it returns None

scale\_factor = 1.05

min\_neighbour = 6

faces = face\_cascade.detectMultiScale(img, scale\_factor, min\_neighbour, minSize=(100, 100),

flags=cv2.CASCADE\_SCALE\_IMAGE)

if len(faces) == 0:

return None

# Crop all faces found

for (x, y, w, h) in faces:

cv2.rectangle(img, (x, y), (x+w, y+h), (0, 255, 255), 2)

cropped\_face = img[y:y+h, x:x+w]

#center\_x=

#center\_y=

center\_x = int(x + w / 2)

center\_y = int(y + h / 2)

pan\_angle = map\_value(center\_x, 0, frame.shape[1], 0, 180)

tilt\_angle = map\_value(center\_y, 0, frame.shape[0], 0, 180)

mirror\_pan\_angle=mirror\_value(pan\_angle)

mirror\_tilt\_angle=mirror\_value(tilt\_angle)

pan\_pin.write(make\_positive(mirror\_pan\_angle))

tilt\_pin.write(make\_positive(mirror\_tilt\_angle))

return cropped\_face

# Doing some Face Recognition with the webcam

video\_capture = cv2.VideoCapture(0)

while True:

\_, frame = video\_capture.read()

face = face\_extractor(frame)

if face is not None:

# Resize the image to match the pretrained model input

face = cv2.resize(face, (224, 224))

im = Image.fromarray(face, 'RGB')

img\_array = np.array(im)

img\_array = np.expand\_dims(img\_array, axis=0)

pred = model.predict(img\_array)

print(pred[:,1])

if pred[:,1] > 0.001:

name = 'Target Found'

else:

name = 'Mask found'

cv2.putText(frame, name, (50, 50), cv2.FONT\_HERSHEY\_COMPLEX, 1, (0, 255, 0), 2)

else:

cv2.putText(frame, "No match", (50, 50), cv2.FONT\_HERSHEY\_COMPLEX, 1, (0, 255, 0), 2)

cv2.imshow('Video', frame)

if cv2.waitKey(1) & 0xFF == ord('q'):

break

video\_capture.release()

cv2.destroyAllWindows()

# code for face detection

import cv2

from deepface import DeepFace

import pyfirmata

face\_cascade = cv2.CascadeClassifier(cv2.data.haarcascades + 'haarcascade\_frontalface\_default.xml')

board = pyfirmata.Arduino('COM5')

pan\_pin = board.get\_pin('d:9:s') # Digital pin 9 for pan servo

tilt\_pin = board.get\_pin('d:10:s') # Digital pin 10 for tilt servo

def mirror\_value(val,):

midpoint = (0 + 180) / 2

mirror\_val = midpoint - (val - midpoint)

return mirror\_val

def make\_positive(n):

if n < 0:

return -n # Return the absolute value

return n

def map\_value(value, from\_min, from\_max, to\_min, to\_max):

return int((value - from\_min) \* (to\_max - to\_min) / (from\_max - from\_min) + to\_min)

def detect\_faces(reference\_img\_path):

cap = cv2.VideoCapture(0, cv2.CAP\_DSHOW)

cap.set(cv2.CAP\_PROP\_FRAME\_WIDTH, 640)

cap.set(cv2.CAP\_PROP\_FRAME\_HEIGHT, 480)

counter = 0

face\_match = False

while True:

ret, frame = cap.read()

if not ret:

break

if counter % 30 == 0: # Process every 30th frame

try:

gray = cv2.cvtColor(frame, cv2.COLOR\_BGR2GRAY)

faces = face\_cascade.detectMultiScale(gray, 1.1, 5)

face\_match = False

for (x, y, w, h) in faces:

if DeepFace.verify(frame[y:y+h, x:x+w], reference\_img\_path)['verified']:

face\_match = True

center\_x = int(x + w / 2)

center\_y = int(y + h / 2)

pan\_angle = map\_value(center\_x, 0, frame.shape[1], 0, 180)

tilt\_angle = map\_value(center\_y, 0, frame.shape[0], 0, 180)

mirror\_pan\_angle=mirror\_value(pan\_angle)

mirror\_tilt\_angle=mirror\_value(tilt\_angle)

pan\_pin.write(make\_positive(mirror\_pan\_angle+40))

tilt\_pin.write(make\_positive(mirror\_tilt\_angle-75))

for (x, y, w, h) in faces:

color = (0, 255, 0) if face\_match else (0, 0, 255)

cv2.rectangle(frame, (x, y), (x+w, y+h), color, 2)

label = "Target" if face\_match else "Non-Target"

cv2.putText(frame, label, (x, y-10), cv2.FONT\_HERSHEY\_SIMPLEX, 0.5, color, 2)

except ValueError:

pass

counter += 1

cv2.imshow("video", frame)

key = cv2.waitKey(1)

if key == ord("q"):

break

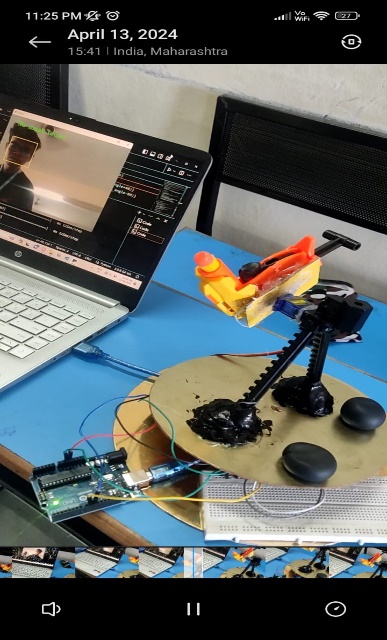
cap.release()

cv2.destroyAllWindows()

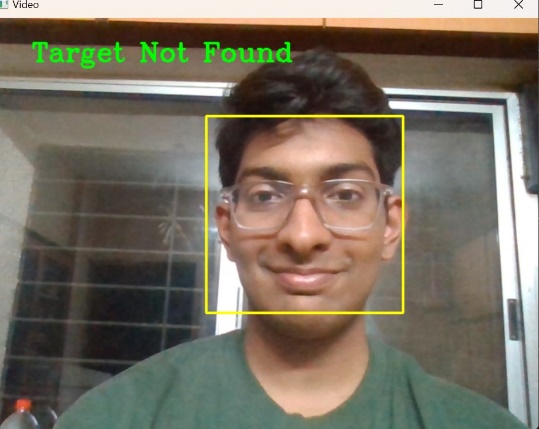
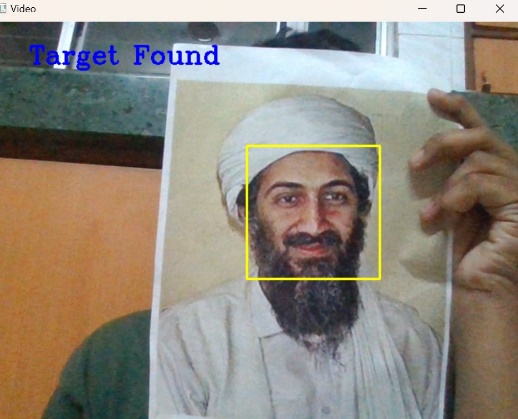
# Usage

detect\_faces(r'C:\Users\Aadesh\Documents\projects\Shooter\reference.jpg')

OUTPUT :  
MODEL :-



DETECTION:-

**CONCLUSION:**

In conclusion, AI GUN represents a transformative advancement in security technology, offering unprecedented capabilities for threat detection, assessment, and response. By leveraging artificial intelligence, computer vision, and machine learning algorithms, AI GUN systems enhance situational awareness, automate security operations, and empower security personnel to effectively mitigate security threats and ensure public safety.

Throughout this report, we have explored the key components, methodologies, challenges, applications, technological advancements, and future directions of AI GUN. We have highlighted its significance in enhancing security measures across various sectors, including public safety, critical infrastructure protection, border security, and event management.

Despite its potential benefits, AI GUN also presents challenges, such as algorithm accuracy, real-time processing requirements, data privacy concerns, and ethical considerations. Addressing these challenges requires a multidisciplinary approach involving expertise in artificial intelligence, cybersecurity, privacy, ethics, and human factors.

Looking ahead, the future of AI GUN holds immense promise, with advancements in autonomous capabilities, multi-modal sensing, predictive analytics, human-centric design, edge intelligence, robustness against adversarial attacks, and collaborative security ecosystems. These advancements will enable AI GUN systems to evolve and adapt to emerging security threats and meet the evolving needs of users in diverse applications and environments.

In summary, AI GUN represents a paradigm shift in security technology, revolutionizing the way we detect, assess, and respond to security threats. By harnessing the power of artificial intelligence, AI GUN has the potential to significantly enhance security measures, protect critical assets, and ensure public safety in an increasingly complex and dynamic world.