FYP Final Report

DEEP LEARNING BASED LASER FENCING

Final Year Project Report

by

Capt Sarosh Ahmed Khan Mughal
Capt Ahmed Umair Khan
Capt Muhammad Awais Malik
Capt Usman Aks-i-Muhammad

Supervisor
Dr. Fahim Arif

In Partial Fulfillment

Of the Requirements for the degree

Bachelor of Engineering in Software Engineering (BESE)

Military College of Signals

National University of Sciences and Technology

Islamabad, Pakistan

(May 2023)

DECLARATION

We hereby declare that this project report entitled “Deep Learning Based Laser Fencing” submitted to the “Department of Computer Software Engineering”, is a record of an original work done by us under the guidance of Supervisor “Dr. Fahim Arif” and that no part has been plagiarized without citations. Also, this project work is submitted in the partial fulfillment of the requirements for the degree of Bachelor of Computer Software Engineering.

Team Members	**Signature**
Capt Sarosh Ahmed Khan Mughal	_____
Capt Ahmed Umair Khan	_____
Capt Usman Aks I Muhammad	_____
Capt Muhammad Awais Malik	_____

Supervisor:	**Signature**
Dr. Fahim Arif	_____

Date:
29 May 2023

Place:
Miliary College of Signals, NUST, Rawalpindi.

DEDICATION

Dedicated to our exceptional parents and supervisor whose tremendous support and cooperation led us to this wonderful accomplishment.

ACKNOWLEDGEMENTS

We are thankful to my Creator Allah Subhana-Watala for guiding us throughout this work at every step and for every new thought which He set up in our mind to improve it. Indeed, we could have done nothing without His priceless help and guidance. Whosoever helped us throughout the course of our thesis, whether our parents or any other individual was His will, so indeed none be worthy of praise but Him.

We are profusely thankful to our beloved parents who raised us when we were not capable of walking and continued to support us throughout every department of our life.

We would also like to express special thanks to our supervisor Dr. Fahim Arif for his help throughout our thesis. Each time we got stuck in something; he came up with the solution. Without his help, we wouldn't have been able to complete our thesis. We appreciate his patience and guidance throughout the whole thesis.

Finally, we would like to express our gratitude to all the individuals who have rendered valuable assistance to our study.

TABLE OF CONTENT

LIST OF FIGURES

ABSTRACT

As security threats have become more sophisticated and traditional physical barriers have become less effective, there has been a growing demand for laser fencing, especially at the borders. It is a versatile and effective security solution that can be adopted to meet a wide range of security needs. This technology is being used around the world for border security, critical infrastructure protection, military bases, prisons, wildlife conservation, and residential and commercial security. Its advanced sensors and deep-learning algorithms make it a highly reliable solution for detecting and preventing intrusions. Its most common applications involve its deployment at such places at the borders where human presence is practically impossible due to difficult terrain or harsh weather conditions. Features like enhanced security, deterrence to criminal activity, cost-effectiveness, scalability, real-time monitoring, and reduced personnel requirements have made this technology an attractive option for border security agencies around the globe.

This paper proposes a solution called Deep-Learning Based Laser Fence that comprises poles fitted with lasers and sensors to detect any intrusion between them. The poles are placed hundreds of meters apart. The system consists of a Transmitter and a Receiver unit, which are constantly talking to each other through data sharing. If an intruder “breaks” the laser beam; an alarm is triggered. Whenever an intrusion is attempted across a particular perimeter, the communication, and the data sharing between the two poles gets disrupted and a pulse is sent to Command Post - the C&C Platform - over the wired communication network. The system constantly evolves using Machine Learning to reduce false positives in case of non-human intrusion and become smarter. Hence, assisting with threat analysis of that perimeter. The build-in algorithm can detect if it is a human or an animal. Even a crawling intruder is also detectable with this software. The solution is designed for use in harsh environments and provides high detection accuracy in all weather conditions. It uses the latest technology which increases detection sensitivity and reduces nuisance alarms. All signals are digitally processed - with proprietary algorithms - which gives maximum detection performance with an extremely low false alarm rate. This ensures a very high security standard is achieved.

Chapter 1

INTRODUCTION

1. Intrusion Detection System (IDS)

A physical Intrusion Detection System (IDS) is a security tool used to identify and prevent unauthorized physical entry into a facility, building, or region [1]. To identify any unauthorized access or incursion attempts, sensors and sirens are frequently used. A physical intrusion detection system can be either active or passive. In an active system, movement or environmental changes are detected using devices like motion sensors, lasers, or infrared sensors. In contrast, a passive system monitors changes in the environment using devices like cameras, microphones, or pressure sensors.

To offer better security and monitoring capabilities, the Internet of Things (IoT) is rapidly being used in intrusion detection systems. Real-time monitoring and alerting capabilities can be added to a physical intrusion detection system by integrating IoT devices, such as sensors, cameras, and alarms. IoT devices can detect a variety of events, including movement, sound, temperature changes, and humidity, and these events can be utilized to set off alarms or alerts. To stop any infiltration attempts or unauthorized access, these devices can be installed in several places, including doors, windows, and walls. One advantage of utilizing IoT in such systems is possessing the capacity to gather and analyze substantial amounts of data. The accuracy of the intrusion detection system can be increased, and false alarms can be decreased by using this data to identify patterns and trends. Additionally, remote monitoring and control capabilities can be offered by IoT devices. As a result, security professionals can monitor the physical intrusion detection system from distant locations and respond appropriately if an intrusion is found.

1.1 Major Components of an Intrusion Detection System (IDS)

An IDS comprises of many components that operate together for detecting any physical intruder and alerting the concerned security staff. The main components of an IDS are

mentioned below [2]:

a. Sensors

The sensors are the first line of defense in an IDS for physical intruders. They are responsible for detecting physical intrusion attempts and collecting data on activity within the protected area. Sensors can be placed at various points throughout the protected area, including at entry points, on fences or walls, and within the interior of the protected area.

b. Analyzers/ Alarms

The analyzers are responsible for analyzing the data collected by the sensors and identifying potential security threats. Analyzers use a set of rules and algorithms to compare the data collected against known patterns of malicious activity and generate alerts when suspicious activity is detected. When a sensor detects a potential security breach, it triggers an alarm. Alarms can be audible, such as a siren or a bell, or silent, such as a notification to security personnel.

c. Control Panel

The control panel, also known as the console, is the user interface for the IDS. It provides a central location for security personnel to monitor and manage alerts generated by the system. The control panel can also provide tools for investigating security incidents and managing the IDS configuration.

d. Response

The response component is responsible for taking action when a security threat is detected. Responses can include dispatching security personnel to investigate the potential security breach, notifying law enforcement or emergency services, or activating security measures such as locking doors or gates.

1.2 Types of Intrusion Detection System (IDS)

To identify and address potential security risks, intrusion detection systems (IDS) come in a variety of forms. They are listed as follows [3]:

a. Perimeter IDS

This type of IDS is designed to detect any unauthorized access to the perimeter of a building or facility. It may use sensors, cameras, or other types of technology installed around the perimeter of a facility to detect intruders, or any attempt to breach a physical boundary like a wall or a fence, etc.

b. Access Control IDS

This type of IDS is integrated with access control systems and is designed to detect any unauthorized entry into a restricted area. By combining access control and intrusion detection systems, Access Control IDS can help organizations protect their physical and digital assets from unauthorized access and other security threats. They can be used to protect buildings, data centers, networks and other critical assets. Access Control IDS mainly include access control devices like security cards, biometric scanners, PIN pads, etc., authentication and authorization servers, intrusion detection sensors, alarm systems, and monitoring and management software.

c. Motion Detection IDS

This type of IDS is designed to detect any movement inside a restricted area. It may use sensors, cameras, or other types of technology to detect intruders. To work, a motion detection IDS typically includes motion sensors, alarm systems, monitoring and management software and might involve integration with other security systems such as perimeter intrusion detection systems, video surveillance systems, access control systems, etc.

d. Glass Break IDS

This type of IDS is designed to detect any breaking of glass windows or doors. It may use acoustic, vibration or shock sensors to detect the sound of breaking glass. This system is commonly used to protect buildings, storefronts, and other areas that have glass windows or doors that can be easily broken. Glass break IDS can be an effective way to detect and deter potential intruders who attempt to gain access by breaking a window or door. By

detecting the sound of breaking glass, this system can trigger alarm and alert security personnel, allowing them to respond quickly and prevent a security breach.

e. Video Analytics IDS

Video Analytics IDS is a kind of intrusion detection system (IDS) that uses cameras to monitor and detect any unauthorized activity or intrusion in a secured area. This technology is frequently employed in locations requiring constant monitoring, such as critical facilities, public spaces, or huge commercial structures. By providing real-time video footage and analytics, this system can help security personnel respond quickly and prevent a security breach.

f. Alarm System

It is a kind of intrusion detection system (IDS) that employs numerous alarms to notify security staff of an infiltration attempt. This system is frequently utilized in houses, buildings, and other locations where a dependable security solution is required. These systems can include audible alarms, visual alarms, or notifications that are triggered when an intrusion attempt is detected.

1.3 Applications of IDS

Physical intrusion detection systems are used to detect unauthorized entry into a defined region or perimeter. They are applied in a variety of industries and settings to improve security and safety. Here are some instances of the application of IDS in various fields [4]:

a. **Military and Defense:** Physical IDS are used to secure military bases, weapons storage facilities, and other high-security areas. They are used to detect intruders and potential threats.

b. **Industrial and Manufacturing:** Physical IDS are used to secure industrial sites and manufacturing plants. They help prevent theft, sabotage, and damage to equipment.

c. **Transportation and Logistics:** Physical IDS are used to secure transportation

infrastructure such as airports, seaports, and rail yards. They help prevent unauthorized access to sensitive areas and cargo.

d. **Healthcare:** These are used to secure hospitals, clinics, and other healthcare facilities. They help prevent unauthorized access to sensitive patient information and medical supplies.

e. **Education:** Physical IDS are used to secure school campuses and other educational facilities. They help prevent unauthorized access to sensitive areas and ensure the safety of students and staff.

f. **Retail:** These IDS are used to secure retail stores and shopping centers. They help prevent theft, shoplifting, and other criminal activities.

g. **Residential:** Such systems are also used to secure private homes and residential communities. They help prevent unauthorized access and enhance personal safety.

h. **Agriculture:** By identifying any unauthorized entrance to a farm or field, an IDS can assist farmers in preventing crop theft. Motion sensors, cameras, or laser detectors can all be used for this.

2. Perimeter Intrusion Detection System (PIDS)

One of the critical aspects of national security is the prevention of unauthorized entry of goods and individuals into a country from its borders [5]. A Perimeter Intrusion Detection System (PIDS) is an effective tool for surveilling and detecting potential threats at borders. It can be employed for detection of various kinds of threats, for example, illegal crossing of borders, smuggling of drugs and weapons, and other illegal activities. Integration of PIDS with different types of sensors like infrared sensors, acoustic sensors, and seismic sensors further enhances the functionality of the system by detecting any activity which might equate to intrusion or infiltration. Typical sensor types for border security PIDS include [6]:

- **Ground Sensors:** Detect any vibration or movement in the ground brought on by a person crawling, walking, or excavating.

- **Microwave Sensors:** Detect any changes in the microwave field caused by someone entering the protected area.

- **Infrared Sensors:** Detect any temperature variations brought on by the movement of people or vehicles.

- **Acoustic Sensors:** Detect any sound or noise that someone crossing the border might have made.

PIDS can be installed all the way along the length of a border to provide capabilities for ongoing surveillance and detection as shown in Figure 1. Applications like border security require real-time information to be provided to the security personnels. Thus, an IDS can be configured with a command-and-control system to provide alerts immediately when an unusual activity occurs which allows the border patrol to respond promptly [7].

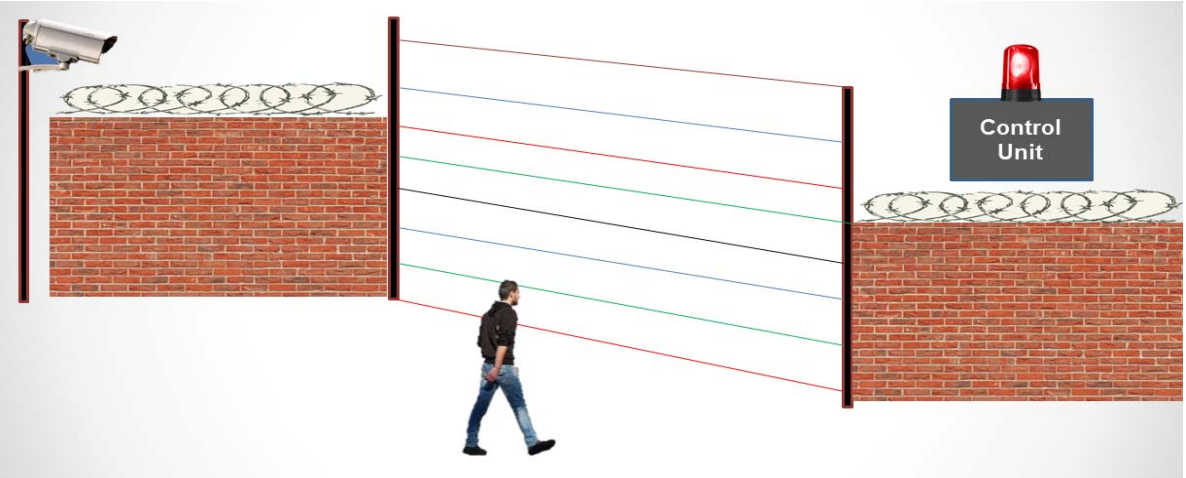


Figure 1. General Working of a Perimeter Intrusion Detection System (PIDS)

Depending on how serious the threat is, the reaction can include sending security guards to

the location, as well as sending in police enforcement or military forces. An IDS does not only monitor the borders, but they can also be trained for the surveillance of large areas including nearby forests, buildings, hills, and potential hideouts of illegal personnels. Such systems can be integrated with other technologies like surveillance cameras to enhance their effectiveness.

In the past, wired security systems were thought to be the most dependable and cost-effective intrusion detection technology [8]. The primary benefit of wired systems is the ease in connecting them to a monitoring service over a phone line. However, if the cables themselves are not sufficiently safeguarded, these systems might be susceptible to tampering, necessitating professional installation. Wireless security systems have grown in popularity because of recent advancements in wireless technology since they are simple to set up, don't require cabling, and can be remotely armed. The drawback of these systems is that each sensor needs an external power source. If batteries are used, they might need to be changed or recharged frequently, especially for security cameras, which might only have a 24-hour battery life.

2.1 Laser Fencing

One of the most effective and affordable methods for security fencing systems is laser technology. Laser fencing is a type of perimeter security technology that uses lasers to build an invisible wall that can both detect and resist potential invaders. Due to its ability to function in a range of weather situations and its ability to cover large areas, laser fence is especially well-suited for border security.

Laser fencing functions by continuously generating a laser beam that forms a fictitious fence along the border. The system recognizes when the beam is broken, such as when a person or vehicle crosses the boundary, and an alert or alarm is set off as a result. Some benefits of using laser fencing for border security include [9]:

- **High accuracy:** Laser fencing is very accurate and can identify even the smallest border crossings.

- **Low false alert rate:** Laser fencing is made to limit false alarms as much as possible, which can assist in lightening the burden for border security officers.

- **Cost-effective:** Laser fencing is less expensive to maintain than conventional physical security systems, making it a good option for border security.

- **Low maintenance:** Laser fencing is a low maintenance option for border protection. It only needs occasional cleaning.

For a complete security solution for border security, laser fences can be combined with other security measures like surveillance cameras. Laser fencing can provide continuous monitoring and detecting capabilities, while minimizing false alarms and lightening the strain for border security personnel. As a result, laser fencing is an effective and efficient solution for border protection.

2.2 Internet-of-Things (IoT) and Smart Laser Fencing

Internet-of-Things (IoT) is a linked network of devices, sensors, and systems that can exchange data and communicate with one another. When paired with smart laser fencing, it can give a sophisticated and all-encompassing perimeter security solution. This integration can improve the laser fencing system's functionality and effectiveness. IoT can improve Smart laser fence in a variety of ways, including [10]:

Sensor integration: IoT sensors can be used in conjunction with smart laser fencing to offer real-time environmental data such as temperature, humidity, and wind speed. This information can be utilized to fine-tune the laser fencing system's sensitivity and increase the system's detecting capabilities.

Video surveillance integration: IoT-enabled cameras can be used with smart laser fencing to give real-time video surveillance of the perimeter. This can be beneficial for detecting

potential security risks as well as providing visual proof of any detected intrusions.

Data analytics: The Internet of Things (IoT) can offer data analytics capabilities that can aid to increase the smart laser fence system's accuracy. The system may learn to distinguish between typical environmental changes and potential security concerns by analyzing the data gathered by IoT sensors.

Remote monitoring and control: The smart laser fence system may be monitored and managed remotely thanks to the Internet of Things (IoT). As a result, security staff can keep an eye on the system continuously from a single location and respond quickly to any incursions they notice.

Chapter 2

LITERATURE REVIEW

In literature, several works are present which discuss the design, development, and use of smart laser fence systems with an emphasis on how internet of things technology might improve the system. The articles go through the advantages of perimeter security utilizing smart laser fencing as well as the difficulties in incorporating IoT into the system. In general, these research articles offer insightful information about the creation and use of smart laser fencing for perimeter security.

The researcher in [11] had put forth a motion detection method that involved subtracting the pixel values from two consecutive image frames and using objects as an analogy. The outcomes of the trials show that the suggested method enables continuous monitoring of object and vehicle movement in video frames. When the researcher adds additional algorithms to this system, it is simple to determine the location and speed of cars. In [12], the tracking, detection, and validation system is used to analyze the variation of two consecutive frames in order to suggest a new method for movement detection. By using pixel basis displacement algorithm in the frame of the object as the actual and anterior, it improved the capability of tracking the movement, with a heavy focus on the development of smart video surveillance systems. In [13] laser security systems were shown to have a high level of technical innovation that improved protection. This project's cheap budget is due to its simple design. The system's qualities may lead to the creation of more conventional protective mechanisms. This system is one of the more economical security system solutions because of technological advancements. [14] demonstrated that the smart web security system is a home-based or office-based security system that can be effective in situations when security is a concern. The movement detector is one of the possibilities for an affordable security system that fills the need for a low-cost security system in daily life. The study in [15] shows that the movement detection principle of the MDSS would result in a lower resource requirement for it to function as intended. The system avoids unnecessary storage by only recording when it detects movement. Additionally, this system alerts and cautions the operator of motion so that he is aware of a site activity. [16]

proposes a novel approach to movement detection with an algorithm. Thus, a system for video surveillance and disclosure was effectively created. The system is primarily outfitted with an effective monitoring technique and is intended to be extremely beneficial for any user or organization. The approach of movement detection is used in [17], which combines the frame variation method with morphological processes, and is used to identify moving objects. The study of the rule of frame variation method and the solution of the numerous issues appears to be the cornerstone of the activity. In [18] each possible background pixel can be selected to carefully update the adaptive background model at each frame. Furthermore, this method also applies the conditional Cauchy models to discover animated objects instead of the single threshold work, thus generating the exact movement mask. [19] suggests smart laser fence technology for border surveillance. The system, which is based on laser beam interruption technology, can accurately detect, and classify a variety of targets, including people and vehicles. The system can be linked with current security systems to create a complete security solution. It uses a combination of hardware and software to achieve continuous and ubiquitous coverage. In [20] a smart laser fence system for safeguarding vital infrastructure is proposed. The device can categorize intruders based on their size and movement patterns and employs laser beams to detect and track them. In case of a breach, the system also has an alarm module to notify security staff. The system can be installed in a variety of locations, including airports, power plants, and military bases, as it is made to be expandable. The study in [21] suggests an Internet of Things-based smart laser fence system for perimeter protection. The system, which is based on laser beams that intruders interrupt, may categorize them according to their size and movement styles. The system also has an IoT module that notifies security staff of breaches and sends alerts to them. The system is made to be scalable and can be used in a range of locations, including apartment buildings, manufacturing facilities, and military stations. Through experimental experiments, we assess the system's functionality and demonstrate that it can reliably identify and categorize intruders in a variety of environmental settings. The suggested system in [22] offers an affordable and dependable perimeter security solution with IoT connectivity. The system's capabilities are improved with the incorporation of IoT technology, which also offers real-time monitoring and control. The system's detection and classification skills will be further improved in the future work, and it will be integrated with other security systems to offer a complete security solution for perimeter protection using

IoT technology. [23] introduced a method for safeguarding huge establishments, including significant enterprises, military bases, and colleges. The typical means for securing these kinds of locations include operator inspection, the installation of barbed wire on walls and borders, and similar measures. However, they also have their own issues. This paper described a method for optical communication using a laser light beam. The model in [24] is intended to safeguard agriculture and keep out both animals and field intruders with bad intentions. According to Gowri (2019), a LASER sensor will increase the security of the field and crops by detecting any object at the boundary itself. Additionally, this will increase the safety of farmers. The main objective of this research is to find crop protection strategies that are both more successful than farmers' present practices and do not directly affect wild animals. [25] suggests a fiber optic sensor-based virtual fence. The virtual fence can recognize the animals due to its intelligence. After the animals have been identified, it can alert the farm owner and send a message to the animals. The machine learning techniques utilized in the smart fence described in the paper are good at recognizing signals specific to people, elephants, and tigers. The smart fence can presently detect people moving around the farmland in addition to identifying certain animals. The optical fiber cable sensor's entire configuration underwent extremely regressive testing. Testing has been done to distinguish between people, tigers, and elephants.

The proposed work presents a deep learning-based laser fencing system that uses laser beam interruption technology to detect any intruder. The system is integrated with a video camera and gets activated only when an object crosses the laser beam. When the occlusion occurs, the camera will turn on and indicate if the beams are cut by a human or any other object including animals, vehicles, etc. The reported work uses a combination of hardware and software to achieve its goals.

Chapter 3

PROBLEM DEFINITION

The issue of protecting particularly big areas, such as sizable institutions, military installations, government departments, and countries with multiple boundaries, is challenging. These facilities are often guarded by operator inspection, the placement of barbed wire at regular intervals along its length, and other methods. However, there are some presumptions and issues with these methods. Operator inspection is only possible to a certain degree. Thieves or saboteurs can cut the barbed wire while utilizing the approach with it. Also, this approach is expensive. Closed-circuit television (CCTV) is far more expensive, undesirable, and impractical to use to monitor borders.

Physical security systems, and more specifically perimeter security, have grown to be crucial in defending today's crucial assets and key resources. The capacity of a PIDS system to retain a high probability of detection (POD) to intrusions while minimizing alerts due to nuisance events, particularly those generated by wind, rain, traffic, or other nuisance activities, is the most crucial performance indicator. Simply raising the POD sensitivity also raises the sensitivity to annoyance occurrences. The PIDS system must be able to adapt to various situations and effectively distinguish between intrusions and nuisances in order to shift the scales in favor of POD. Being able to automatically adapt to changing conditions is a crucial feature since it eliminates the need for routine system adjustment. PIDS systems are becoming increasingly sophisticated thanks to recent developments in AI and other intelligent signal and data processing approaches.

There is no one technology that can completely solve the problem of guarding a perimeter. Only a small portion of a bigger security program and solution exists in the form of a perimeter intrusion detection system. Using a multi-layered strategy that combines a physical barrier (fence), CCTV cameras, access control, and perimeter incursion detection is the key to perimeter security.

Pakistan shares a border with four countries and has a total land border length of 6,774 kilometers [26]. It is practically impossible to install CCTV cameras and set up Check-Posts after every few meters in the disputed and vulnerable regions. Also, in difficult and rough terrains deploying military becomes a challenging task. This work proposes a deep learning-based laser fencing system that minimizes the requirement of human involvement and is a very cost-effective solution.

Chapter 4

METHODOLOGY

4.1 Overview of the methodology

The Laser Fencing detection project methodology consists of a methodical approach for designing, creating, deploying, and testing a Laser Fence system. The process is separated into following stages:

- **Research Phase:** During this phase, the project team will conduct research to better understand the concept of Laser Fencing technology and its components. Find online tools that can contribute in the project. Furthermore, the team will do market research to identify existing Laser Fence systems and their properties.

- **Design Phase:** Using the findings of the research, the project team will develop a Laser Fence system that can adapt to different terrains and weather conditions. The design will include the hardware and software components of the system, as well as the detection mechanism and alarm system.

- **Development Phase:** During this phase, the project team will design the hardware and software components of the Laser Fence system. The hardware components will include lasers, sensors, and alarms, while the software components will include system control and data processing.

- **Assembly and Calibration Phase:** Following the development of the hardware and software components, the project team will construct and calibrate the Laser Fence system to ensure exact detection.

- **Testing Phase:** During this phase, the project team will test the Laser Fence system in a range of locations and weather conditions to ensure its effectiveness and durability. The team will also evaluate the system's cost-effectiveness and compare it to other security systems on the market.

- **Evaluation and Improvement Phase:** Based on the test results and evaluation, the project team will identify any problems and chances for improvement. Following that, the team will deploy the required system modifications and retest the system to ensure that it meets the appropriate standards.

The procedure will be deliberate and iterative, with each step building on the one that came before it. The approach will also entail collaboration between the project team and key stakeholders to ensure that the system meets the requirements and expectations of the users.

4.2 Flow Chart for the Working of the Proposed System

The architectural design of the Deep Learning Based Laser Fencing is **Event Driven Architecture.** Upon the detection of an event, the system acts accordingly. Python and embedded C Language are used which notifies the system whenever a LOS block by some object and python using trained model will try to identify the incoming threat. This project keeps monitoring the targeted area 24/7 and when the intruder crosses through the laser fence it gets activated and the camera screen pops up on the screen and gets the live streaming with the detection of the intruder.

4.3 Sequence Diagram of the Proposed System

The sequence diagram shows the sequence of events. The intruder when trying to cross laser fencing will be notified to the main system. That will turn the camera on and pop up the camera window on the screen. Crossing will also generate a specific alarm and the camera will try to detect the intruder position on the screen.

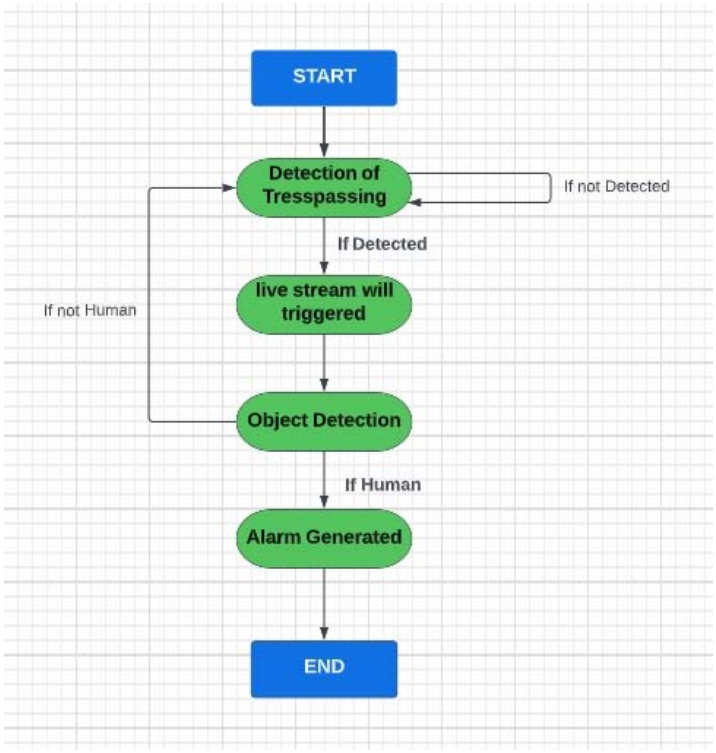


Figure 2. Event-Driven architecture of Deep - Learning Based Laser Fencing

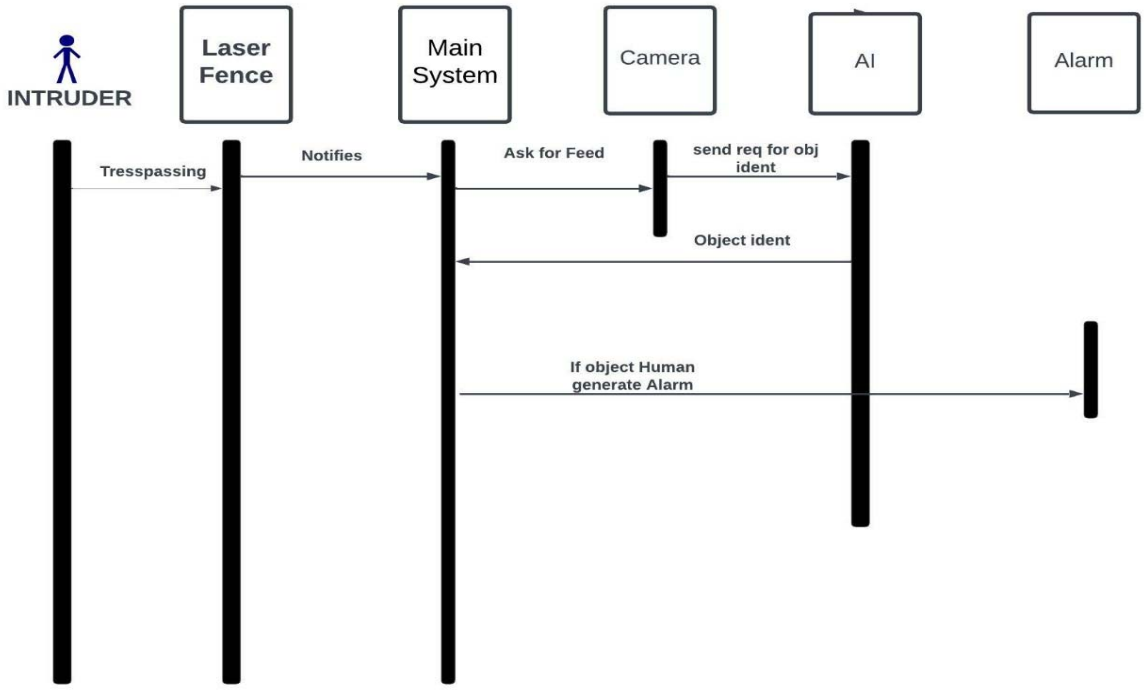


Figure 3. Sequence Diagram of Deep - Learning Based Laser Fencing

4.4 The Detection Mechanism

The Laser Fence system's detecting method is a critical component of the project. The detection device oversees detecting any incursion into the laser-created virtual barrier. The detecting method is made up of numerous parts, including sensors, alerts, and software. The sensors are set along the virtual barrier that the laser beams have built. The sensors are intended to detect any interference in the laser beams generated by an item or a person. When an incursion is detected, the sensors transmit a signal to the alarms, which causes an audible and visual warning to be sent. The alerts are intended to be very visible and loud for security staff to react quickly to any suspected incursion. The software oversees managing and interpreting data from sensors and alarms. The program captures sensor data and saves it in a database. The program may also create reports and give useful information on the facility's security. To detect any entry properly, the detection mechanism of the Laser Fence system should be very sensitive and accurate. To limit the frequency of false alerts, the detecting method should also have a low false alarm rate. To limit the frequency of false alerts triggered by animals or environmental variables, the detecting method should be able to discriminate between objects and people.

Chapter 5

DETAILED DESIGN AND ARCHITECTURE

5.1 System Architecture

The Laser Fence Project is an effective event-driven system that can detect and recognize trespassing objects, record video footage, and generate an alarm in case of human trespassing. Its partitioning of responsibilities ensures that each component of the system performs its specific function, resulting in a more efficient and effective system. The system architecture is shown in Figure 7.

Figure 4. Architecture of the laser fencing system

5.1.1 The functionalities of system components

The system comprises three main components:

The Laser Fence: The laser fence consists of two metallic rods. One rod is loaded with five Lasers and the other rod is loaded with five photodiodes. The Lasers and the photodiodes are aligned at the same levels. The Lasers are semiconductor devices that are continuously emitting Infrared radiation. Lasers only emit light when they are given a power supply of 5 Volts. These diodes are passive semiconductor devices and become active only when they are exposed to light, including infrared radiation. When the beam of light is interrupted, the circuit becomes open and it sends a signal to the microcontroller board, Arduino Nano, which triggers the camera to turn on and capture the scene if a human is detected.

Figure 5. (a) Photodiode component

Figure 5. (b) Photodiode in working mode

Figure 6. Infrared (IR) Laser to Generate Laser Beam

The Camera: The camera is connected to a microcontroller board i.e., Arduino Nano which is responsible for the serial communication between the laser fence and the main system integrated with camera. We have used Opencv library in Python. The primary function of OpenCV (Open-Source Computer Vision) is to provide a set of tools and algorithms for computer vision and machine learning applications. Some of the key functions of OpenCV include image processing, feature detection, object recognition, etc.

The Alarm System: The alarm system is incorporated in the Python code which generates an alarm in case of human trespassing. The alarm can be a buzzer, a siren, or any other type of alarm that can be easily heard. We have used siren audio as alarm sound.

Chapter 6

IMPLEMENTATION AND TESTING

6.1 Implementation

Implementing deep learning-based laser fencing involves several steps, including hardware setup, data collection, model training, and deployment. Here's a brief overview of the steps involved:

Hardware Setup: The first step in implementing a laser fence is to set up the hardware, including laser emitters and receivers. The laser emitter sends a beam of light, and the receiver detects any interruption in the beam caused by an object passing through the laser fence.

Data Collection: Once the hardware is set up, data needs to be collected for training the deep learning model. This involves capturing images and video of objects passing through the laser fence from different angles and distances.

Data Preprocessing: The collected data needs to be preprocessed before it can be used for training the deep learning model. This includes tasks such as data cleaning, normalization, and image augmentation to improve the quality and diversity of the data.

Model Training: The next step is to train a deep learning model on the preprocessed data. This involves selecting an appropriate architecture, such as a convolutional neural network (CNN), and fine-tuning the model using transfer learning.

Model Evaluation: Once the model is trained, it needs to be evaluated on a separate test dataset to assess its accuracy and performance. This involves metrics such as precision, recall, and F1 score.

Deployment: Once the model is trained and evaluated, it can be deployed for real-world use. This involves integrating the model with the hardware, such as the laser emitter and receiver, and implementing a user interface for monitoring and controlling the system.

6.1.1 Hardware Setup

The design of the Laser Fence system is critical to the project's success. The system will have numerous hardware components such as the laser source, sensors, alerts, etc. The primary design concerns for each component are as follows:

- **Laser Source:** The most important component of the Laser Fence system is the laser source. The laser source creates a light beam that is employed to build the virtual fence. Even in inclement weather, the laser source should be strong enough to provide a clear and distinct beam of light. It should also be accurate and precise to guarantee that the laser beam is unbroken. The laser source used in this project is IR Laser.

- **Sensors:** Sensors detect any interruptions in the laser beam. Photoelectric, infrared, and ultrasonic sensors are all options. To detect any trespass precisely, the sensors must be exceedingly sensitive and accurate. This project uses photo diodes which perform the task of a sensor.

- **Alarms:** Alarms are used to notify security staff of any possible entry. Alarms may be either audible or visual, or both. Alarms should be very visible and loud for security staff to react quickly.

- **Camera:** The camera is responsible for recording the video feed and sending it to the microcontroller board. It is also responsible for processing the video feed using OpenCV to detect and recognize the trespassing object. If the trespassing object is a human, the camera triggers the alarm system.

6.1.2 Generating Data Set

Generating datasets is crucial in developing accurate and effective machine learning and

AI models, especially in situations where relevant data may not be readily available or where data needs to be tailored to a specific use case. Generation of data sets is essential for improving model accuracy, domain specific data, customized data, overcoming data scarcity, addressing bias, etc. For our project, we generated the dataset by installing a google chrome extension “Download All Images”. This extension is a tool that allows users to download all the images quickly and easily on a web page. We used this tool to get a zip file of all the images obtained as a result of searching “human” and “person” on Google.

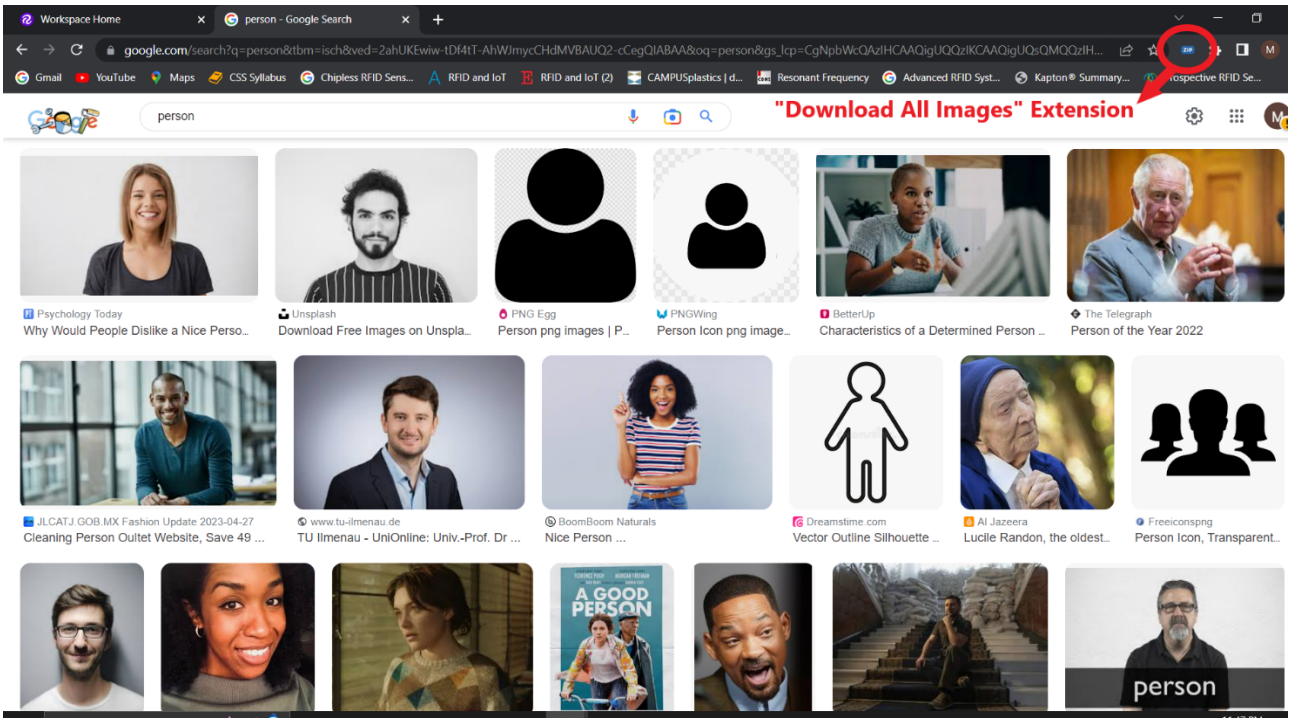


Figure 7. Google Search Results for “Person” to Generate Data Set

6.1.3 Assembling the Data Set – Annotation

We have used “Roboflow” to annotate the data set obtained in the first step. Roboflow is an online platform that provides tools for managing, annotating, and transforming datasets for computer vision tasks such as object detection, segmentation, and classification. It is designed to streamline the process of creating and managing datasets, allowing developers and data scientists to focus on building machine learning models. Additionally, Roboflow offers integrations with popular machine learning frameworks such as TensorFlow, PyTorch,

and Keras, allowing users to seamlessly integrate their datasets into their machine learning workflows.

In this step, we will upload the data set obtained from google images on Roboflow for annotation. Annotation refers to the process of labeling or adding metadata to raw data. It is a crucial step in preparing data for machine learning models and other artificial intelligence applications. Data annotation involves adding information such as tags, keywords, or other types of metadata to help categorize or classify data. In this project, we have annotated the images with the tag “person”.

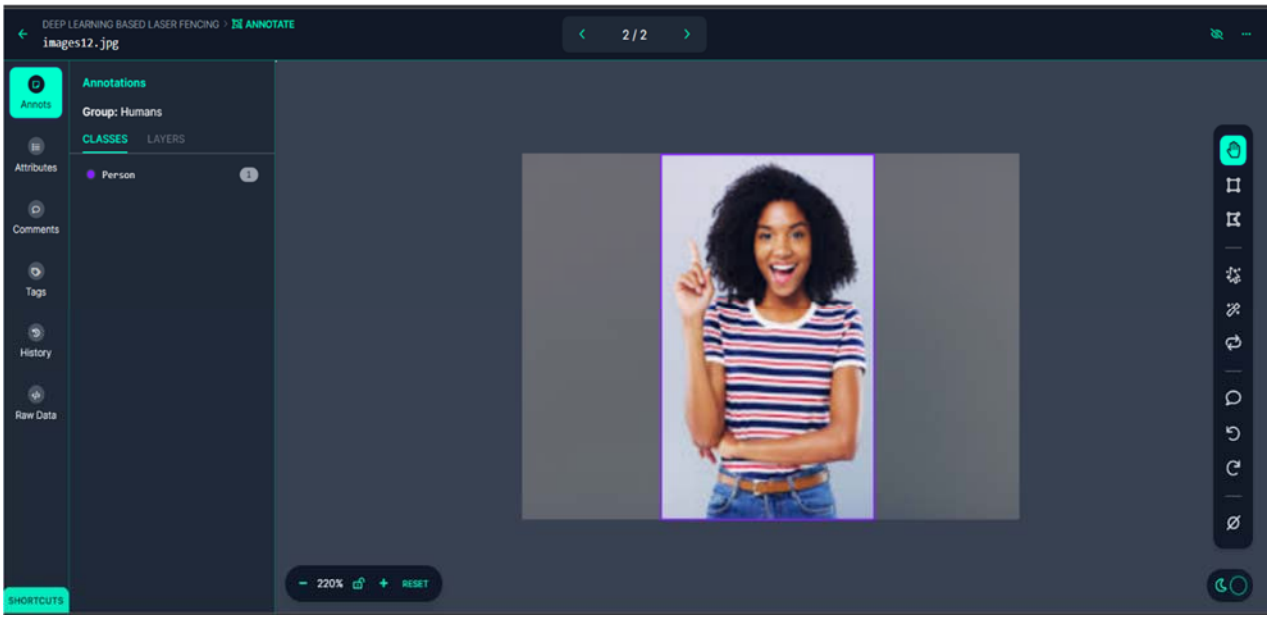


Figure 8. Annotation of the Data Set Obtained from Google Images in Step 1

6.1.4 Augmentation

The next step after annotating the images is the augmentation of the data set. Data augmentation is a technique used in machine learning and deep learning to increase the size and diversity of training datasets by generating new synthetic data from existing data. The goal of data augmentation is to improve the accuracy, robustness, and generalizability of machine learning models by exposing them to a wider range of data variations. Data augmentation techniques typically involve applying transformations or manipulations to the

existing data, such as:

1. Flipping or rotating images
2. Changing the brightness, contrast, or color of images
3. Adding noise or distortions to images
4. Cropping or resizing images
5. Adding or removing parts of images

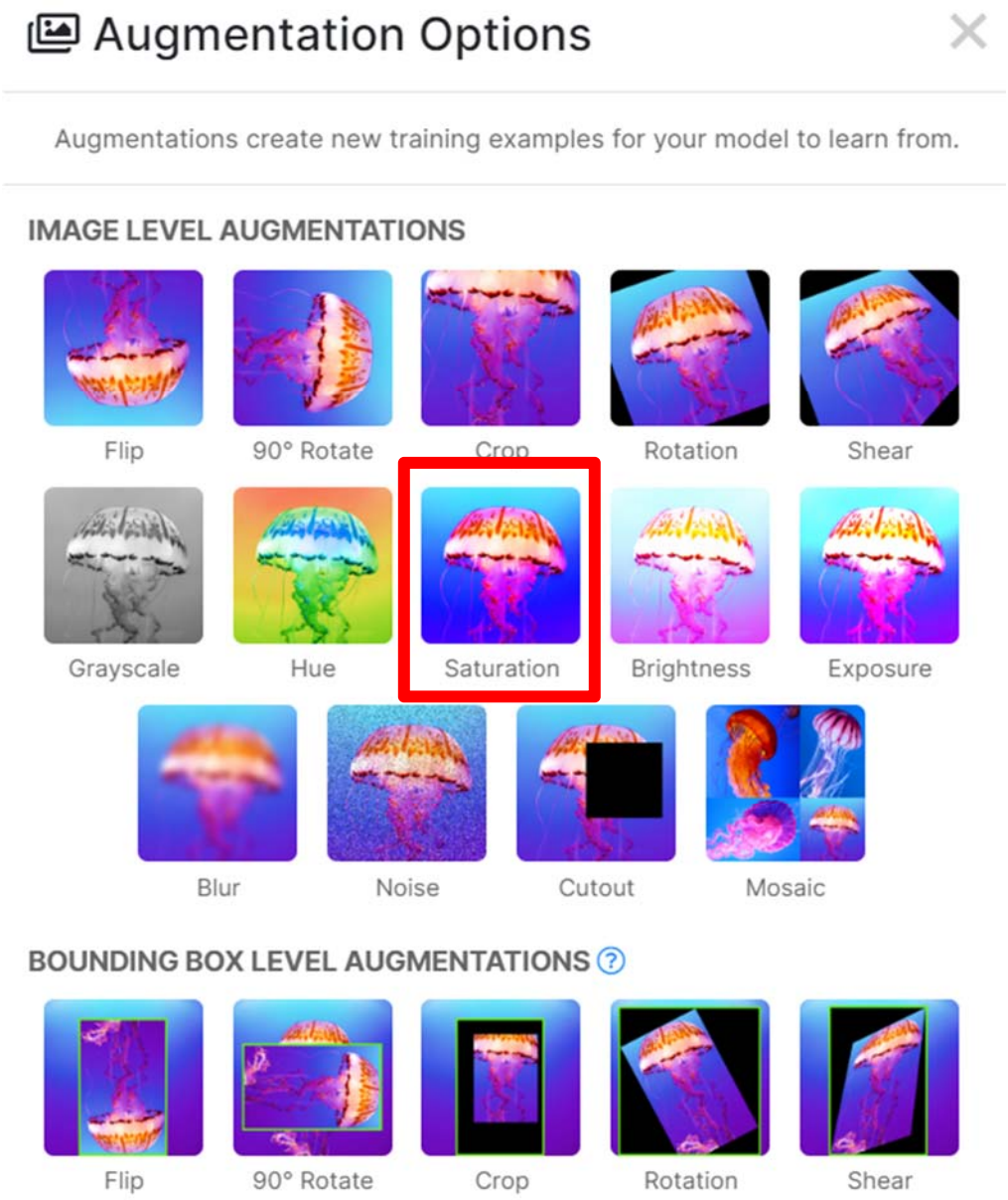


Figure 9. Augmentation Options Available in Roboflow

We have applied “Saturation” augmentation on the data set. Saturation augmentation involves adjusting the color saturation of an image to create variations in the dataset. Color saturation refers to the intensity of colors in an image. An image with high saturation will have bright and vivid colors, while an image with low saturation will have more muted colors.

6.1.5 Custom Training with YOLOv5

Generating custom datasets can help in creating models that are tailored to specific use cases, resulting in more accurate predictions. Google Colaboratory, also known as "Colab", is a free cloud-based platform for running and sharing Jupyter notebook-style projects. It is provided by Google and is a part of the Google Cloud Platform. Colab allows users to run Python code and perform data analysis, machine learning, and deep learning tasks using popular libraries such as TensorFlow, Keras, PyTorch, and OpenCV. It provides a GPU and TPU runtime, allowing users to train models much faster than using a local machine. Roboflow provides us with a snippet which we have further used to train our model using Colab.

```
[2]  !python train.py --img 416 --batch 16 --epochs 150 --data {dataset.location}/data.yaml --weights yolov5s.pt --cache
```

Figure 10. Arguments Passed for Extraction of Image Features

We can pass several arguments here, including the input image size defined by "img", the batch size determined by "batch", and the number of training epochs defined by "epochs". It is common to use 3000 or more epochs for training. The location of our dataset is saved in "data.location". To start transfer learning from the generic COCO pretrained checkpoint, we specify a path to weights with "weights". We can also cache images for faster training using "cache". Epochs is a very important parameter in model training. In machine learning, "epochs" refers to the number of times a learning algorithm will iterate over the entire training dataset during the training process. In other words, each epoch represents one complete pass through the training data. During each epoch, the learning algorithm updates the model parameters based on the error or loss function calculated on the training data. This is how the model will be trained. After the model has been trained, we have performed

inference on the images in the test/images folder using a pre-trained checkpoint obtained from Roboflow. In custom training models using YOLOv5, the MAP (Mean Average Precision) is commonly used as an evaluation metric to assess the performance of the model in object detection tasks. During training, YOLOv5 calculates the detection metrics (including mAP) on the validation set after each epoch. This metric is used to evaluate how well the model performs on object detection and to help tune the model's hyperparameters, such as learning rate and data augmentation. The MAP for our model is 0.93. After our model is trained, the YOLOv5 custom training will provide us with a .pt file which we have named “multipleIntruders.pt”. This is our trained model.

6.1.6 AI Processing

For AI processing of the model, we have used Python 3.10. The Python Script is as follows:

```
#Importing the necessary libraries

from playsound import playsound

import torch

import cv2

import serial

import os

import datetime

# Get the current date and time as a string

now = datetime.datetime.now().strftime('%Y-%m-%d_%H-%M-%S')

import numpy as np

import winsound

# Define the codec and create a VideoWriter object
```

```
fourcc = cv2.VideoWriter_fourcc(*'mp4v')

now = datetime.datetime.now().strftime("%Y-%m-%d_%H-%M-%S")

out = cv2.VideoWriter(f'C:/Users/Sarosh/Desktop/recording/output_{now}.mp4', fourcc, 20.0, (640, 480))



duration = 300 # milliseconds

freq = 750  # Hz

i = 0

# Defining the line thickness and width, height of the image

# Defining the x coordinates of the lines and the image path

line_thickness = 4

width, height = 800, 600

xx1 = 40

xx2 = 140

path = r'images/Gate.png'



# Setting up the serial communication with Arduino

arduino = serial.Serial('COM4', 9600,timeout=.1 )

state = 1

states = 0



# Starting the webcam capture
```

```
cap = cv2.VideoCapture(0)

# Initializing variables to store the received digit values

digit5 = 0

digit4 = 0

digit3 = 0

digit2 = 0

digit1 = 0

colour5 = (0, 0, 255)

colour4 = (0, 0, 255)

colour3 = (0, 0, 255)

colour2 = (0, 0, 255)

colour1 = (0, 0, 255)



# Loading the custom YOLOv5 model

model = torch.hub.load('yolov5', 'custom', path='MultipleIntruders.pt', source='local',)



# Create blank image for overlay

overlay = np.zeros((height, width, 3), dtype=np.uint8)

# Looping through the code continuously until stopped

while True:

    # Reading the data received from the Arduino
```

```
    if arduino.in_waiting > 0:
        data = arduino.readline().decode().strip()
        digit5, digit4, digit3, digit2, digit1 = map(int, data)
        print(f"Received data: {digit5}{digit4}{digit3}{digit2}{digit1}")
    # Setting up the fence status image and drawing the lines based on the received digit values
    if digit1 == 1:
        colour5 = (128,128,128)
        state = 0
    if digit2 == 1:
        colour4 = (128,128,128)
        state = 0
    if digit3 == 1:
        colour3 = (128, 128, 128)
        state = 0
    if digit4 == 1:
        colour2 = (128, 128, 128)
        state = 0
    if digit5 == 1:
        colour1 = (128, 128, 128)
        state = 0
    if state == 1:
```

```
img = cap.read()[1]

image = cv2.imread(path)

cv2.line(image, (xx1, 70), (xx2, 70), colour1, thickness=line_thickness)

cv2.line(image, (xx1, 120), (xx2, 120), colour2, thickness=line_thickness)

cv2.line(image, (xx1, 170), (xx2, 170), colour3, thickness=line_thickness)

cv2.line(image, (xx1, 220), (xx2, 220), colour4, thickness=line_thickness)

cv2.line(image, (xx1, 270), (xx2, 270), colour5, thickness=line_thickness)


cv2.putText(image, "L1", (10, 75), cv2.FONT_HERSHEY_PLAIN, 1, (0, 0, 255), 2)

cv2.putText(image, "L2", (10, 125), cv2.FONT_HERSHEY_PLAIN, 1, (0, 0, 255), 2)

cv2.putText(image, "L3", (10, 175), cv2.FONT_HERSHEY_PLAIN, 1, (0, 0, 255), 2)

cv2.putText(image, "L4", (10, 225), cv2.FONT_HERSHEY_PLAIN, 1, (0, 0, 255), 2)

cv2.putText(image, "L5", (10, 275), cv2.FONT_HERSHEY_PLAIN, 1, (0, 0, 255), 2)

# Resize both frames to have the same height

height = min(img.shape[0], image.shape[0])

framez = cv2.resize(img, (int(img.shape[1] * height / img.shape[0]), height))

imagez = cv2.resize(image, (int(image.shape[1] * height / image.shape[0]), height))

# Combine both frames horizontally

combined_frame = cv2.hconcat([framez, imagez])

# Write the combined frame to the video file

out.write(img)
```

```
        # Show the combined frame in the window
        cv2.imshow('Combined', combined_frame)
        if cv2.waitKey(1) & 0xFF == ord('q'):
            break
    if state == 0:
        img = cap.read()[1]
        image = cv2.imread(path)
        result = model(img)
        df = result.pandas().xyxy[0]
        for ind in df.index:
            x1, y1 = int(df['xmin'][ind]), int(df['ymin'][ind])
            x2, y2 = int(df['xmax'][ind]), int(df['ymax'][ind])
            label = df['name'][ind]
            conf = df['confidence'][ind]
            text = label + ' ' + str(conf.round(decimals=2))

            if float(conf.round(decimals= 2)) >= 0.5:
                if label == 'person':
                    print("Human")
                    cv2.rectangle(img, (x1, y1), (x2, y2), (0, 0, 255), 2)
                    cv2.putText(img, text, (x1, y1 - 5), cv2.FONT_HERSHEY_PLAIN, 2, (0, 0,
255), 2)
```

```
                winsound.Beep(freq, duration)
                # Take a snapshot and save it with the name "intruder" in the PC
                snapshot = img[y1:y2 , x1:x2 ]
                cv2.imwrite(f"C:/Users/Sarosh/Desktop/intruderimage/intruder_{now}.jpg",
snapshot)
                states = 1


        cv2.line(image, (xx1, 70), (xx2, 70), colour1, thickness=line_thickness)
        cv2.line(image, (xx1, 120), (xx2, 120), colour2, thickness=line_thickness)
        cv2.line(image, (xx1, 170), (xx2, 170), colour3, thickness=line_thickness)
        cv2.line(image, (xx1, 220), (xx2, 220), colour4, thickness=line_thickness)
        cv2.line(image, (xx1, 270), (xx2, 270), colour5, thickness=line_thickness)
        cv2.putText(image, "L1", (10, 75), cv2.FONT_HERSHEY_PLAIN, 1, (0, 0, 255), 2)
        cv2.putText(image, "L2", (10, 125), cv2.FONT_HERSHEY_PLAIN, 1, (0, 0, 255), 2)
        cv2.putText(image, "L3", (10, 175), cv2.FONT_HERSHEY_PLAIN, 1, (0, 0, 255), 2)
        cv2.putText(image, "L4", (10, 225), cv2.FONT_HERSHEY_PLAIN, 1, (0, 0, 255), 2)
        cv2.putText(image, "L5", (10, 275), cv2.FONT_HERSHEY_PLAIN, 1, (0, 0, 255), 2)
        # Resize both frames to have the same height
        height = min(img.shape[0], image.shape[0])
        framez = cv2.resize(img, (int(img.shape[1] * height / img.shape[0]), height))
        imagez = cv2.resize(image, (int(image.shape[1] * height / image.shape[0]), height))
        # Combine both frames horizontally
```

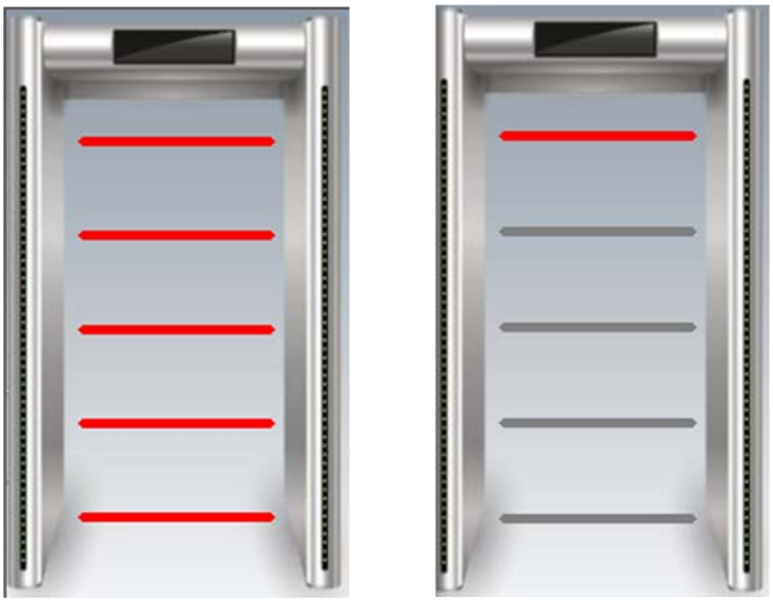
```
combined_frame = cv2.hconcat([framez, imagez])
# Write the combined frame to the video file
out.write(img)
# Show the combined frame in the window
cv2.imshow('Combined', combined_frame)
if cv2.waitKey(1) & 0xFF == ord('q'):
    break
i+=1
print(i)
if i > 50:
    colour1 = (0, 0, 255)
    colour2 = (0, 0, 255)
    colour3 = (0, 0, 255)
    colour4 = (0, 0, 255)
    colour5 = (0, 0, 255)
    datas = 0
    i = 0
    state = 1
    states = 0
```

According to this code, when there is no obstruction between the two poles, the connection between the Laser and the Photodiode is shown by the red lines as portrayed by Figure 11. As soon as someone or something passes between the poles, the laser beam gets distorted, and

the camera starts detecting the object. If it is identified as a person, it generates a siren which informs the security personnel deployed with the system to take the necessary action. Also, the person will only be identified if their confidence level is above 0.5.

6.1.7 Serial Communication with Hardware

We have used Arduino Nano for serial communication between the software and the hardware. Arduino IDE 1.8.13 has been used to write a C-code to program the board.



(a) (b)

Figure 11. Visual representation of light being emitted from the Laser source when there is: (a) no obstruction (b) obstruction.

When there is some obstruction in the laser beams, the Arduino reads the signal and transmits it to the main system where AI processing is done. The C program for serial communication is given as:

```
int buttonPin1 = 8;
int buttonState1 = 0;
```

```
int buttonPin2 = 7;
int buttonState2 = 0;

int buttonPin3 = 6;
int buttonState3 = 0;

int buttonPin4 = 5;
int buttonState4 = 0;

int buttonPin5 = 4;
int buttonState5 = 0;

void setup()
{
  Serial.begin(9600);
  pinMode(buttonPin1, INPUT);
  pinMode(buttonPin2, INPUT);
  pinMode(buttonPin3, INPUT);
  pinMode(buttonPin4, INPUT);
  pinMode(buttonPin5, INPUT);
}

void loop()
{
  int newButtonState1 = digitalRead(buttonPin1);
  int newButtonState2 = digitalRead(buttonPin2);
  int newButtonState3 = digitalRead(buttonPin3);
  int newButtonState4 = digitalRead(buttonPin4);
  int newButtonState5 = digitalRead(buttonPin5);

  if (newButtonState1 != buttonState1 ||
```

```
    newButtonState2 != buttonState2 ||
    newButtonState3 != buttonState3 ||
    newButtonState4 != buttonState4 ||
    newButtonState5 != buttonState5) {

  Serial.print(newButtonState1);
  Serial.print(newButtonState2);
  Serial.print(newButtonState3);
  Serial.print(newButtonState4);
  Serial.println(newButtonState5);

  buttonState1 = newButtonState1;
  buttonState2 = newButtonState2;
  buttonState3 = newButtonState3;
  buttonState4 = newButtonState4;
  buttonState5 = newButtonState5;
 }

 delay(1);
}
```

6.2 Testing

Testing of the developed project is done by placing different objects in front of the camera and checking whether it is able to distinguish between humans and other objects or not. The algorithm is developed such that if the confidence level is below 0.5, the camera will not annotate the object and alarm will not be triggered. It is evident from the following figures that when anything, which is not a human, is cutting the light beam as indicated by gray lines in the figures, the camera is not identifying them as their confidence level is below 0.5. When a person obstructs the light beams, it detects them as a human along with their confidence

level and generates an alarm.

Figure 12. When a bag distorts the laser beams.

6.2.1 Test Cases

Test cases for a laser fence system are:

System's ability to detect intruders: This test case involves simulating the presence of an intruder within the laser fence system and verifying that the system is able to detect the intrusion and trigger an alarm.

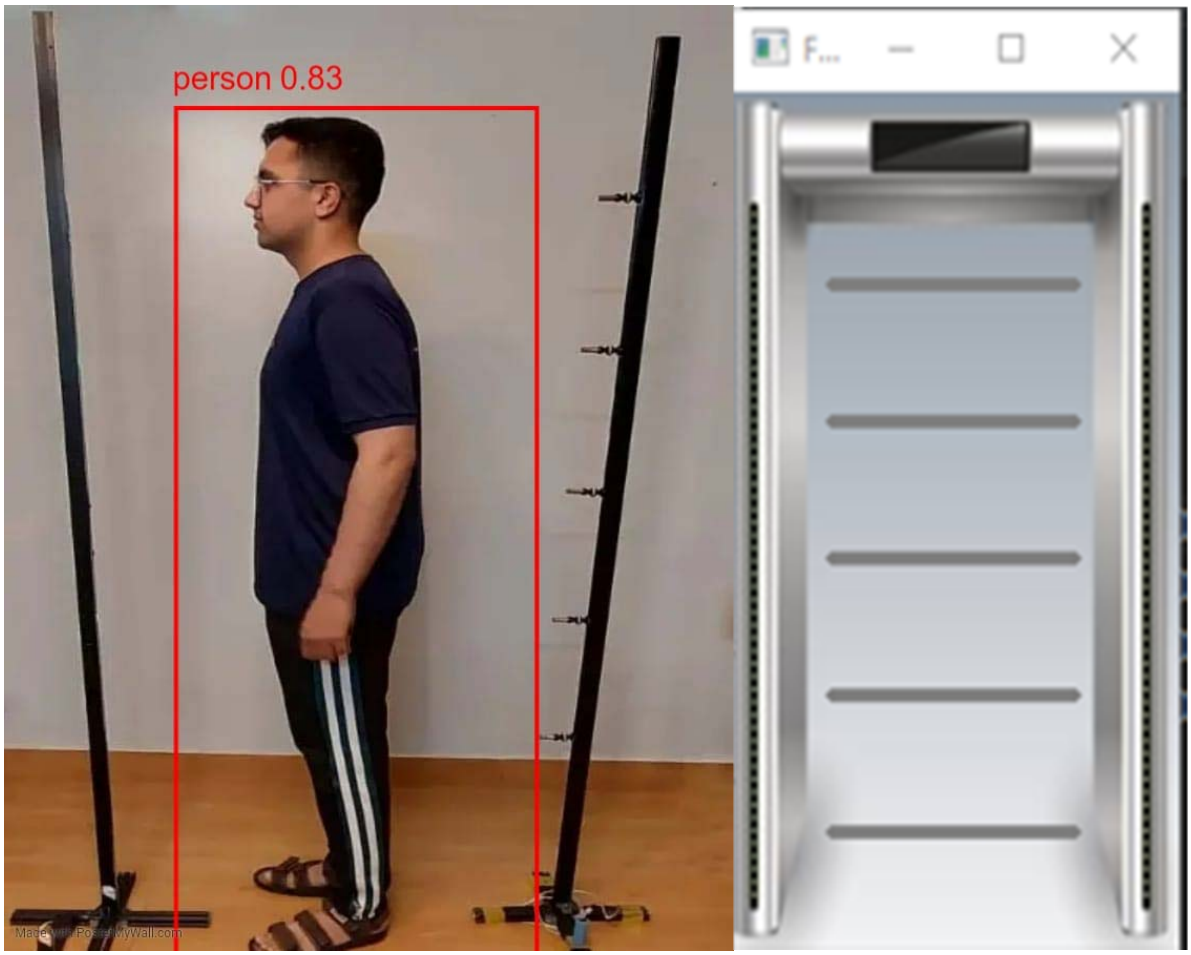


Figure 13. When a human crosses the fence (side view).

System's ability to distinguish between intruders and other objects: This test case involves introducing various objects (e.g., animals, debris) into the laser fence system and verifying that the system is able to distinguish between these objects and human intruders.

System's response time: This test case involves measuring the time it takes for the system to detect an intruder and trigger an alarm. The response time should be within a specified range.

System's ability to handle different weather conditions: This test case involves subjecting the system to various weather conditions (e.g., rain, snow, fog) and verifying that it is able to

function properly under these conditions.

System's ability to handle different light conditions: This test case involves subjecting the system to various light conditions (e.g., bright sunlight, low light) and verifying that it is able to function properly under these conditions.

System's ability to handle false alarms: This test case involves introducing various types of interference (e.g., animals, debris) into the laser fence system and verifying that the system is able to distinguish between false alarms and actual intrusions.

System's durability: This test case involves subjecting the system to various physical stresses (e.g., impact, vibration) and verifying that it is able to withstand these stresses and continue functioning properly.

System's ability to communicate with external devices: This test case involves verifying that the system is able to communicate with external devices (e.g., security cameras, alarms) and trigger appropriate actions.

Chapter 7

RESULTS AND DISCUSSION

From the data collected in the implementation and the testing phase, it is evident that the proposed project has a MAP of 0.93 which is a common performance metric used to evaluate object detection models. A MAP score of 0.93 indicates that the model has a high level of accuracy in detecting objects in the images it was trained on. The following figures indicate that a person is identifiable even if his back is facing towards the camera or if he is crawling through the fence or manipulating the fence.

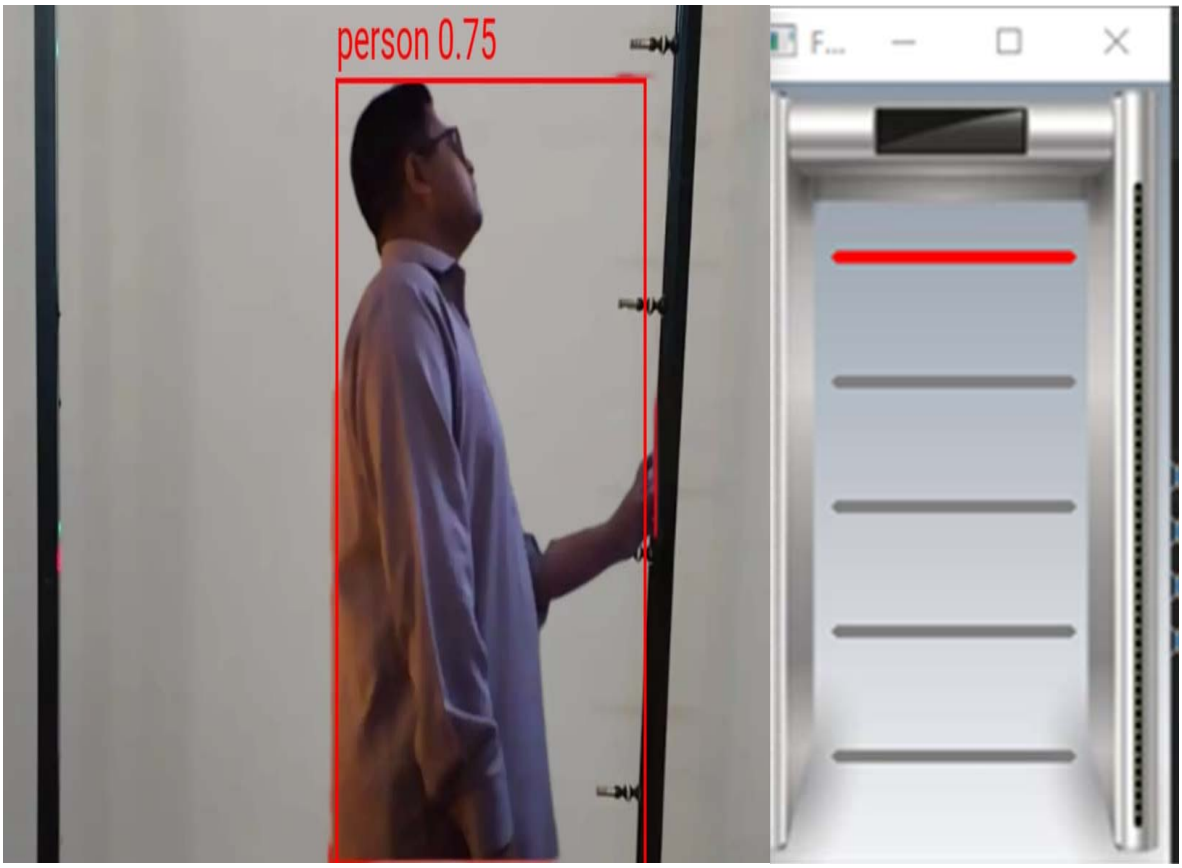


Figure 14. A person manipulating the fence

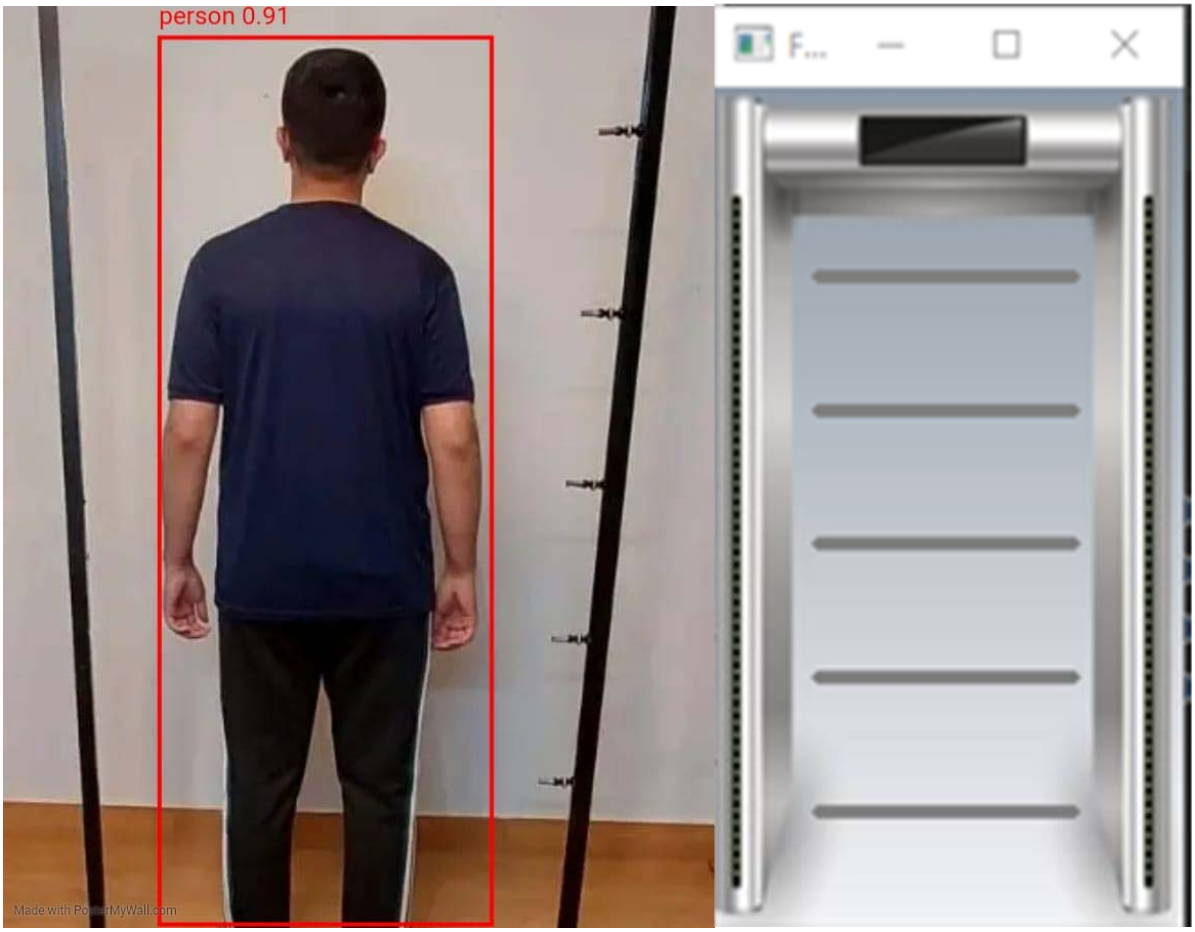


Figure 15. A person facing with his back towards the camera detected with confidence level 0.91

The efficiency of this project can be evaluated by the following factors:

- **Detection accuracy:** The accuracy of object detection is an important factor in determining the efficiency of a laser fencing system. A deep learning model with a high level of accuracy will be more effective in detecting intrusions and reducing false alarms. The trained model of the proposed project has a MAP of 0.93 which shows that it has a high level of accuracy when identifying objects. Also, it is evident from the above figures that it detects humans with a very high confidence level.

- **Response time:** The response time of the system is another important factor in determining its efficiency. A system that can detect and respond to intrusions quickly

will be more effective in preventing breaches and minimizing damage. The proposed system has a very quick response time as it detects an intruder within one second.

- **Cost-effectiveness:** The cost-effectiveness of the system is an important consideration, as it determines the feasibility of deploying the system on a larger scale. The proposed system is very cost-effective and requires minimal maintenance which makes it efficient in the long run.

Chapter 8

CONCLUSION AND FUTURE WORK

8.1 Conclusion

A laser fence system can be an effective solution for protecting large areas such as farmlands, industrial sites, or borders. The laser fence system works by creating a virtual barrier that uses laser beams instead of physical fencing to detect and deter intruders.

The system typically consists of several components, including a control unit, laser sensors, and an alarm system. The laser sensors emit beams of light that create a virtual fence around the perimeter of the protected area. If an intruder crosses the fence, the beam is interrupted, and an alarm is triggered, alerting security personnel to the breach.

A laser fence system can be particularly useful in situations where a physical barrier such as a wall or fence is not practical or desirable. For example, in some industrial or military settings, it may be important to maintain an open perimeter for logistical or strategic reasons. In such cases, a laser fence system can provide an effective way to monitor the perimeter and detect any unauthorized access attempts.

Additionally, the laser fence system is an automated system; it can operate around the clock, providing continuous monitoring and protection. This can be especially useful in situations where physical security personnel may not be available or where human error or fatigue may be a concern.

A laser fence system can be a valuable tool for addressing physical security concerns, providing an additional layer of protection for a variety of settings and applications.

However, it's important to note that a laser fence system may not be suitable for all situations. For example, it may not be effective in areas with heavy fog, rain, or snow, which can interfere with the laser beams. Additionally, the system may require regular maintenance to ensure that the sensors are functioning correctly and that false alarms are minimized.

8.2 Future Developments

The laser fence system technology is continuously evolving, and there are several

potential future developments and improvements that could enhance its effectiveness and applications.

Increased accuracy and sensitivity: Future advancements in laser fence system technology may lead to improved accuracy and sensitivity, allowing for even better detection and deterrence of intruders. This could involve the use of more advanced sensors, algorithms, and machine learning techniques to better differentiate between legitimate and unauthorized access attempts.

Integration with other technologies: The laser fence system may be integrated with other security technologies, such as drones, autonomous vehicles, or robots, to provide a more comprehensive security solution. This could allow for more rapid response times and enhanced situational awareness.

Enhanced versatility: Future laser fence systems may be more versatile, with the ability to adjust to different environments and applications. This could involve developing systems that are better suited for urban or suburban settings, or that can be easily adapted to different topography and terrains.

Improved cost-effectiveness: As the technology matures, the cost of laser fence systems may decrease, making them more accessible to a wider range of applications and settings.

Integration with AI: The laser fence system may be integrated with AI technology to improve its performance and effectiveness. For example, AI algorithms could be used to analyze data from the system and identify patterns and trends that may indicate potential security threats.

Improved detection and tracking: Future laser fence systems may use more advanced sensors and algorithms to improve the detection and tracking of potential intruders. For instance, they could use advanced cameras, artificial intelligence, and machine learning to identify and track intruders more accurately.

Increased range and coverage: Future advancements in laser technology could lead to lasers that are more powerful and have a longer range, allowing for wider coverage of the protected area. This could increase the effectiveness of the system, making it suitable for larger areas.

Reduced false alarms: False alarms can be a significant problem for laser fence systems. Future developments may involve the use of more advanced sensors and algorithms to reduce false alarms, leading to more reliable and effective security.

Adaptability to different environments: Laser fence systems may be developed to be more adaptable to different environments, such as urban or suburban settings, or different topographies and terrains. This could make the technology more accessible and effective for a wider range of applications.

Enhanced mobility: Future laser fence systems may be designed to be more mobile, allowing for rapid deployment and repositioning as needed. This could be useful for temporary events, such as concerts or sporting events, or for military or law enforcement operations.

Chapter 9

REFERENCES

[1] J. J. Zhang, Y. J. Zhao, and S. L. Chen, "A laser-based perimeter security system," in Proceedings of the International Conference on Computer and Communication Technologies, Beijing, China, 2010, pp. 484-487.

[2] J. Y. Kim, J. W. Lee, and J. H. Park, "A laser-based intrusion detection system using fiber-optic sensors," IEEE Sensors Journal, vol. 11, no. 3, pp. 610-616, 2011.

[3] S. P. Singh and P. S. Rana, "Development of laser-based perimeter security system using microcontroller," International Journal of Scientific and Engineering Research, vol. 4, no. 8, pp. 1640-1644, 2013.

[4] H. C. Park, J. H. Choi, and S. K. Kang, "Design and implementation of a laser-based perimeter security system," in Proceedings of the IEEE Conference on Consumer Communications and Networking, Las Vegas, NV, USA, 2014, pp. 101-105.

[5] R. A. Ghani, N. A. Latiff, and N. A. Manap, "Laser fence: An advanced security system," in Proceedings of the IEEE Symposium on Computer Applications and Industrial Electronics, Penang, Malaysia, 2015, pp. 111-115.

[6] S. S. Patil and S. M. Katkar, "Laser-based perimeter security system with wireless communication," International Journal of Innovative Research in Science, Engineering and Technology, vol. 6, no. 4, pp. 4854-4859, 2017.

[7] M. F. A. Rahman, A. H. M. Z. Alam, and M. R. Islam, "Development of a laser-based perimeter security system," in Proceedings of the International Conference on Electrical, Computer and Communication Engineering, Cox's Bazar, Bangladesh, 2018, pp. 1-6.

[8] S. P. Singh and P. S. Rana, "Design and development of laser-based perimeter security system using FPGA," International Journal of Research in Engineering and Technology, vol. 7, no. 4, pp. 44-50, 2018.

[9] H. J. Lee and C. H. Kim, "Development of a laser-based perimeter security system using an optical fiber sensor," Sensors, vol. 19, no. 13, p. 2902, 2019.

[10] M. G. Jafar and M. R. Hossain, "Design and implementation of a laser-based perimeter security system using raspberry pi," in Proceedings of the International Conference on Electrical, Computer and Communication Engineering, Cox's Bazar, Bangladesh, 2020, pp. 1-5.

[11] Mandeep Singh, (2010), “Improved Morphological Method in Motion Detection”, International Journal of Computer Applications (0975-8887), 5, 5-8.

[12] Neelam Patel, (2012), “Motion Detection based on Multi Frame Video under Surveillance System”, International Journal of Emerging Technology and Advanced Engineering, 2, 124-129.

[13] Diponkar Paul, Md. Shohel Rana, Md. Mokarram Hossain, (2012), “A preview on experimentation on Laser security system, IRACST”- Engineering Science and Technology: An International Journal (ESTIJ), 2, 359-366.

[14] Cynthia Tuscano, Blossom Lopes, Stephina Machado, Pradnya Rane, (2013), “Smart Web Cam Motion Detection Surveillance System”, International Journal of Modern Engineering Research (IJMER), 3, 1169-1171.

[15] Sani Aminu, Ibrahim Muhammed Abba, Bashir Isa Dodo, Mia Torres-Dela Cruz, Umapathy Eaganathn, (2013), “Motion Detection Security System (MDSS) in Live video stream”, Proceeding of the International Conference on Artificial Intelligence in

Computer Science and ICT (AICS 2013), 188-197

[16] Lavanya M.P., (2014), “Real Time Motion Detection Using Background Subtraction Method and Frame Difference”, International Journal of Science and Research (IJSR), 3, 1857-1861.

[17] Nishu Singla, (2014), “Motion Detection Based on Frame Difference Method”, International Journal of Information & Computation Technology, 4, 1559-1565.

[18] P.S.S.M. Lalitha Devi, S. Srividya, (2015), “BMM Based Cauchy Distribution (BMMC) Method for Motion Detection”, International Journal of Emerging Engineering Research and Technology, 3, 86-92.

[19] F. Sun, Q. Zhang, and H. Sun, (2015), "Development of a smart laser fence system for border surveillance", Journal of Sensors.

[20] N. Kumar and S. S. Rathore, (2018),"Smart laser fence system for critical infrastructure protection", Proceedings of the IEEE International Conference on Advanced Networks and Telecommunications Systems.

[21] G. S. Kulkarni and S. P. Patil, (2019), "Smart laser fence system for perimeter security using IoT", International Journal of Innovative Technology and Exploring Engineering.

[22] M. M. Tariqul Islam and M. A. Mannan, (2020), "Design and development of smart laser fence with IoT integration for perimeter security", International Journal of Advanced Computer Science and Applications.

[23] R. Ildarabadi, and Z. Keramat, (2022), "Improved laser beams-based security fence to protect borders," J. Appl. Res. Electr. Eng., vol. 1, no. 1, pp. 50-58.

[24] Jilin Daxue Xuebao (Gongxueban), (2022), “An Invisible Fence: Laser Fencing System for Protecting Crops.”, Journal of Jilin University (Engineering and Technology Edition), ISSN：1671-5497, Vol: 41 Issue: 09-2022.

[25] Suman, P.; Singh, D.K.; Albogamy, F.R.; Shibee,M, (2021), “Harnessing the Power of Sensors and Machine Learning to Design Smart Fence to Protect Farmlands.” Electronics, 10, 3094.

[26] Geography: The borders of Pakistan: https://www.dawn.com/news/884966/geographytheborders-of-pakistan