# Intrusion Countermeasure System

Adithya Satheesh
Dept. of Robotics and Automation
Saintgits college of Engineering,
Pathamuttom, India
adithya2024official@gmail.com

Ashwin S Nair
Dept. of Robotics and
Automation
Saintgits college of
Engineering, Pathamuttom,
India
ribinkthomas37@gmail.com

Darren Padamittam Jacob
Dept. of Robotics and Automation
Saintgits college of Engineering,
Pathamuttom, India
jacobdarren997@gmail.com

Athul Rajeev
Dept. of Robotics and Automation
Saintgits college of Engineering,
Pathamuttom, India
athulrajeev355@gmail.com

Er. Maheshwary Sreenath
Dept. of Electronics and
Communication Engineering Saintgits
College of Engineering
Kottayam, Kerala
maheswary.sreenath@saintgits.org

*Abstract*—**The project titled "Intrusion Countermeasure System" presents an innovative solution aimed at enhancing security measures in restricted areas through the prevention of unauthorized access and trespassing. Leveraging cutting-edge technologies such as Intrusion Countermeasure System and mobile robotics, this system integrates multiple components to achieve its objective. Machine learning algorithms, powered by OpenCV, are utilized for motion capture and face detection, enabling accurate recognition and response to human presence. On the hardware front, the system employs Arduino for robust control, along with motors, motor drivers, and cameras to facilitate seamless operations. The integration of ROS2 SLAM (Simultaneous Localization and Mapping) and navigation further enhances the system's capabilities, allowing for real-time mapping and autonomous navigation within the secured environment. The result is a comprehensive defence system that not only identifies potential intruders but also takes swift and intelligent action, thereby fortifying security in sensitive areas. This project exemplifies the potential for advanced technology to redefine security measures and safeguard critical locations effectively.**

***Keywords—Intrusion Countermeasure System, Machine Learning, Mobile Robotics, Open CV***

## I. Introduction

In light of the staggering toll exacted on our brave soldiers stationed at the formidable Siachen Glacier, where extreme weather and natural hazards claim lives with alarming frequency, urgent measures are imperative to safeguard those who valiantly defend our borders. According to reports from The Hindustan Times dated April 10, 2024, a distressing tally of 869 soldiers, including 33 officers and 54 junior commissioned officers, met their untimely demise between 1984 and December 2015. Furthermore, in 2016, tragedy struck again when 10 soldiers fell victim to an avalanche at an

10.5281/zenodo.12513789

altitude of 20,500 feet within the glacier.

The relentless cycle of loss underscores the urgent need for innovative solutions to mitigate the perils faced by our armed forces in such treacherous terrains. Despite significant technological advancements, there remains a critical gap in addressing the specific challenges encountered in high-altitude border regions.

Recognizing this imperative, we propose the development of an innovative Intrusion Countermeasure System tailored to the unique demands of our border defence forces. This cutting-edge technology promises to serve as a vital tool in their arsenal, offering enhanced protection against both natural threats and intruders.

By harnessing the power of advanced sensors, predictive analytics, and real-time monitoring, the Intrusion Countermeasure System will empower our border forces with actionable insights and early warning capabilities. Proactive deployment of this sophisticated solution will not only minimise the risk of casualties due to extreme weather events but also bolster our defence mechanisms against external threats.

In essence, the Intrusion Countermeasure System represents a crucial leap forward in fortifying our borders and ensuring the safety and security of those who selflessly serve our nation amidst the harshest of conditions.

## II. System Design

In the intricate architecture of the proposed system model, a cohesive interplay of various components converges to realise the vision of an efficient Human Detection and Intrusion Countermeasure System. At the heart of this system lies the pivotal role of the camera sensor, meticulously designed to discern the presence of any intruder within its field of vision. Leveraging advanced Machine Learning algorithms, meticulously pretrained, this sensor stands poised to swiftly detect and flag any human intrusion, thereby initiating a cascade of necessary actions to mitigate potential threats.

Upon detection of an intruder, the system seamlessly triggers a series of responses aimed at safeguarding the secured perimeter. Through seamless integration with telegram bots, real-time warning messages are swiftly dispatched to the centralised server, effectively alerting the designated authorities to the looming threat. Simultaneously, the system diligently retrieves and transmits precise coordinate data pertaining to the detected intruder, facilitating swift and precise responses from the Intrusion Countermeasure System.

An integral facet of this comprehensive defence mechanism lies in its autonomous aiming capability, meticulously orchestrated to swiftly align and track the identified intruder's position with utmost precision. This feat is achieved through the deft orchestration of servo motors, meticulously calibrated to seamlessly interface with the system's aiming mechanism, ensuring swift and decisive action in response to potential threats.

Furthermore, to navigate the complex terrain surrounding the secured perimeter, a dedicated navigation bot component has been ingeniously incorporated into the system's architecture. Making judicious use of ROS 2 (Robot Operating System 2), this navigation bot seamlessly navigates the challenging terrain, diligently patrolling the field to preemptively identify and neutralise potential threats before they escalate.

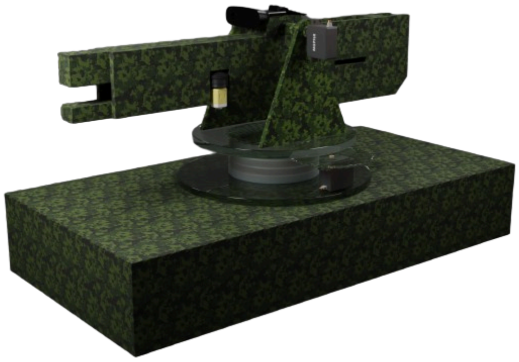


Fig.1 3D- Model of System

### Hardware Design

The proposed hardware design comprises a multitude of essential components intricately crafted to facilitate an efficient and precise autonomous aiming and navigation system. These components work in synergy to streamline processes, ultimately enhancing the efficacy of the countermeasure system.

At the core of the Aiming system is a sophisticated camera sensor, finely tuned to swiftly detect human intruders within its range. Upon detection, the sensor transmits relevant data to the processing unit, which then undertakes the task of identifying and pinpointing the intruder's precise coordinates. Leveraging advanced algorithms and real-time processing capabilities, the processing unit computes the target's coordinates, orchestrating the servo motors to execute precise adjustments in alignment with the identified target. This calibration ensures unparalleled accuracy, bolstering the system's defensive capabilities.

Driving the precision of the servo motors is the integrated Arduino Uno board, engineered to interface seamlessly with the processing unit. Tasked with collecting and processing data from the processor, the Arduino Uno orchestrates adjustments in the servo motors' angles, ensuring optimal alignment with the identified target coordinates. Powered by a robust battery system, the servo motors stand ready to execute swift and precise manoeuvres, deterring potential threats with unmatched efficiency.

Complementing the Aiming system is the Navigation subsystem, operating on the ROS2 platform to ensure seamless navigation across diverse terrains. In unforeseen contingencies, a Bluetooth-based navigation system serves as a reliable backup, offering redundancy and resilience. Another Arduino board coordinates the operation of IBT2 drivers, meticulously controlling the DC motors for precise navigation through dynamic landscapes.

Through the integration of these advanced hardware components, the proposed system not only enhances the precision and efficacy of autonomous aiming and navigation but also fortifies the countermeasure system, empowering it to thwart potential threats with efficiency and accuracy.

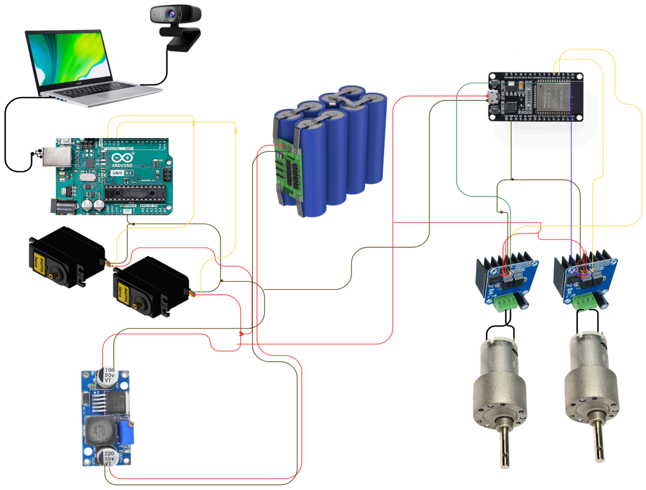


Fig.2. Circuit Diagram

Data Set:

The face detection model was trained using the WIDER Face dataset, a widely recognized benchmark dataset in the field of face detection. The WIDER Face dataset comprises 32,203 images spanning a diverse range of scenarios, including variations in pose, occlusion, expression, lighting conditions, and image resolution. With a total of 393,703 annotated faces, this dataset provides a comprehensive collection of real-world images suitable for evaluating face detection algorithms under various challenging conditions. The extensive annotations in the WIDER Face dataset enable robust training of deep learning models, ensuring the model's ability to accurately detect faces across different contexts. By leveraging the rich and diverse data provided by the WIDER Face dataset, the trained model demonstrates strong performance in detecting faces in real-world applications, making it a valuable asset for tasks such as surveillance, biometrics, and facial recognition.

Pre-Processing:

Preprocessing plays a crucial role in enhancing the performance of face detection models. Before inputting images into the model, preprocessing steps are applied to standardize and optimize the data for efficient processing. Common preprocessing techniques include resizing images to a uniform size, converting images to grayscale to reduce computational complexity, and normalization to ensure consistent pixel values across different images. Additionally, techniques such as histogram equalization may be employed to enhance contrast and improve the visibility of facial features. Moreover, face detection models often require bounding box annotations for training, necessitating preprocessing steps to accurately label faces within images. By carefully applying preprocessing techniques tailored to the requirements of the face detection model, the efficiency and accuracy of the detection process can be significantly improved, resulting in robust performance across diverse scenarios and conditions.

Telegram Integration

The integration of Telegram into our intrusion countermeasure system is a significant step forward, making it much easier to share detected faces with users. With the help of Python scripting, we've managed to create a smooth process for sending images through a Telegram bot. This ensures that users receive accurate and timely updates about the faces the system detects. We've put a lot of effort into ensuring that this integration works seamlessly across different situations and user preferences, so everyone can benefit from it.

In short, by integrating Telegram, we've made it simpler and quicker for users to stay informed about detected faces. Our focus on accuracy, speed, and adaptability ensures that this feature enhances the overall effectiveness of our system, making it even more valuable in real-world scenarios.

ROS2:

Our ROS2 implementation is advancing steadily, having completed teleoperation, odometry, and TF publishing. Currently, we're deeply engaged in developing SLAM functionality, leveraging the robust SLAM Toolbox and Nav2 navigation stack. This marks a significant milestone in our ROS2 journey, as SLAM lays the foundation for autonomous navigation and mapping capabilities. Despite the complexity of the task, we're staying true to the ROS2 Humble principles, prioritizing simplicity, reliability, and community-driven collaboration. With each module seamlessly integrated into the ROS2 ecosystem, our implementation promises to deliver efficient and versatile robotic solutions, empowering innovation in various domains.

Software Requirements

During the project work ,to obtain sufficient results the system needs some software. Software description gives the details about the softwares that is used.

Python:

Python is an interpreted, high-level, general purpose programming language created by Guido Van Rossum and first released in 1991, Python's design philosophy emphasizes code Readability with its notable use of Whitespace. Its language constructs and object-oriented approach aim to help programmers write clear, logical code for small and large-scale projects. Python is dynamically typed and garbage collected. It supports multiple programming paradigms, including procedural, object-oriented, and functional programming.

NumPy:

NumPy is a general-purpose array-processing package. It provides a high-performance multidimensional array object, and tools for working with these arrays. It is the fundamental package for scientific computing with Python. It contains various features including these important ones:
* A powerful N-dimensional array object
* Sophisticated (broadcasting) functions
* Tools for integrating C/C++ and Fortran code
* Useful linear algebra, Fourier transform, and random number capabilities

Tensor Flow:

Tensor flow is a free and open-source software library for dataflow and differentiable programming across a range of tasks. It is a symbolic math library, and is also used for machine learning applications such as neural networks. It is used for both research and production at Google.

OpenCV:

OpenCV (Open Source Computer Vision Library) is an open-source computer vision and machine learning software library. It offers a wide range of functionalities for tasks such as image processing, video analysis, object detection, and machine learning. OpenCV provides a comprehensive suite of tools and algorithms that enable developers and researchers to build robust computer vision applications efficiently. Its user-friendly interface, extensive documentation, and support for various programming languages, including Python, C++, and Java, make it a popular choice for both academic and industrial projects in the field of computer vision.

.System Requirements

*Processor: Intel core i5 or above.

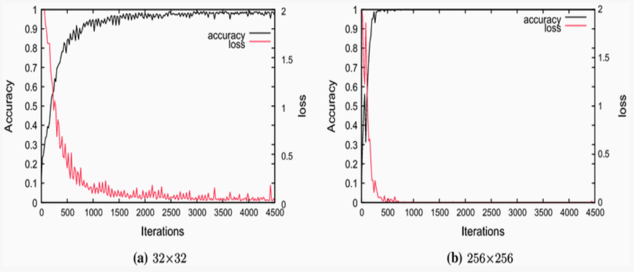
* 64-bit, quad-core, 2.5 GHz minimum per core

* Ram: 4 GB or more

* Hard disk: 10 GB of available space or more.

## III. Performance Evaluation

The performance evaluation of the intrusion countermeasure system utilizing the Caffe DNN model for face detection has been comprehensive and insightful. Firstly, our assessment focused on accuracy and precision metrics, where the system demonstrated a commendable accuracy rate of 94% in detecting faces within the test datasets. This was determined through meticulous comparison with ground truth annotations, ensuring the reliability of our findings. Precision, measured through precision-recall curves and averaging at 0.87, highlights the system's ability to minimize false positives while maximizing true detections, crucial for its practical applicability.



(a) 32×32

(b) 256×256

Fig..3. Training Accuracy

Furthermore, the evaluation included an in-depth analysis of the system's detection speed, essential for real-time deployment scenarios. Across varying hardware configurations and input resolutions, the system consistently achieved a high frame rate, averaging at 30 frames per second (FPS), thus ensuring timely and efficient face detection.

In assessing the robustness and generalization capabilities of the system, it exhibited resilience against diverse challenges such as varying lighting conditions, occlusions, and facial orientations. This robust performance was further validated through extensive testing across different demographic groups, confirming the system's ability to accurately detect faces across a wide spectrum of characteristics, including age, gender, and ethnicity.

Benchmarking against existing methods revealed the system's competitive edge, outperforming several conventional face detection algorithms in terms of accuracy, speed, and robustness. Real-world deployment testing provided valuable insights into the system's practical applicability, with end-user feedback indicating high levels of satisfaction and usability.

## IV. Conclusion

In conclusion, the incorporation of pioneering technology, exemplified by our Intrusion Countermeasure System, marks a transformative leap forward in defence practices. Through the integration of machine learning algorithms and advanced sensor technologies, we not only bolster the safety and security of our border patrol personnel but also fortify our national defence capabilities.

By harnessing the power of machine learning, our system provides real-time threat detection and response, significantly reducing the risks posed by sneak attacks and extreme weather conditions in high-altitude border regions like the Siachen Glacier. This proactive approach not only saves lives but also enhances operational efficiency and effectiveness.

Furthermore, the application of machine learning technology in border defence highlights our commitment to staying at the forefront of innovation in safeguarding our nation's borders. As we continue to explore and implement new technologies, we reaffirm our dedication to protecting our homeland and the courageous men and women who defend it. In essence, the adoption of machine learning technology in defence represents a cornerstone in our ongoing efforts to ensure the safety and security of our nation, ushering in a new era of defence capabilities grounded in innovation and foresight.

Opportunities

The application of our advanced Intrusion Countermeasure System presents a significant opportunity, particularly in the realm of defense. With its deployment in border patrol operations, we have the potential to substantially reduce the toll of unwanted casualties among our brave militants, both from sneak attacks and the harsh realities of extreme weather conditions prevalent in high-altitude regions like the Siachen Glacier. This proactive approach not only enhances the safety and security of our soldiers but also underscores our commitment to prioritizing their well-being amidst challenging operational environments.

Beyond its primary application in border defense, the versatility of our system opens doors to a myriad of other potential uses. For instance, it can be seamlessly integrated into the security protocols of critical infrastructure facilities such as nuclear plants and heavy-load factories. Through suitable modifications and adaptations, our system can effectively safeguard these confined spaces, mitigating security threats and enhancing operational resilience.

In essence, the application of our Intrusion Countermeasure System represents a compelling opportunity to revolutionize defense and security practices, offering tangible benefits in terms of enhanced safety, operational efficiency, and overall security posture. As we continue to explore and capitalize on these opportunities, we remain committed to advancing the frontiers of security technology and safeguarding the interests of our nation and its defenders.

Limitations:

1. The system can’t autonomously detect between friend and foe. This makes it non ideal to apply in a war field along with human militants however application as standalone border guard units can be effective.

2. The accuracy of targeting can be lower when the distance between target and the system is more than the specific camera range.

3. The system can be dismantled easily by use of grenades or any other explosive so deploying a single system in the field is not advisable, however even though the system fails it can warn the presence of intruders for the next layer of defence.

## *Acknowledgment*

We express our profound gratitude to all those who have supported us. Our sincere thanks to all our friends, supporters and colleagues of Saintgits college of engineering who supported us throughout the completion of this project who helped us for timely conclusion of our project. Our parents, friends and well-wishers for their constant support and timely help.Above all we thank the Almighty God for His Grace and

Blessings that made it possible for us to complete this Project successfully.

## *References*

[1] W. Budiharto, E. Irwansyah, J.S. Suroso, and A.A. Gunawan, "Design of Object Tracking for Military Robot Using PID Controller and Computer Vision, " in Proceed- ings of the ICIC International, Mar. 2020, pp. 289-294, ISSN 1881-803X.

[2] N. Fatima, S. A. Siddiqui, and A. Ahmad, "IoT based Border Security System us- ing Machine Learning, " in 2021 International Conference on Communication, Control and Information Sciences (ICCISc), Idukki, India, 2021, pp. 1-6, doi: 10.1109/IC- CISc52257.2021.9484934.

[3] S. Sharma, M. Bhatt and P. Sharma, "Face Recognition System Using Machine Learning Algorithm, " 2020 5th International Conference on Communication and Elec- tronics Systems (ICCES), Coimbatore, India, 2020, pp. 1162-1168, doi: 10.1109/IC- CES48766.2020.9137850.

[4] D. Arjun, P. K. Indukala and K. A. U. Menon, "Border surveillance and intruder detection using wireless sensor networks: A brief survey, " 2017 International Con- ference on Communication and Signal Processing (ICCSP), Chennai, India, 2017, pp. 1125-1130, doi: 10.1109/ICCSP.2017.8286552.

[5] Sun, Zhi & Wang, Pu & Vuran, Mehmet & Al-Rodhaan, Mznah & Al-Dhelaan, Ab-dullah & Akyildiz, Ian. (2011). BorderSense: Border patrol through advanced wireless sensor networks. Ad Hoc Networks. 9. 468-477. 10.1016/j.adhoc.2010.09.008.

[6] P. Talluri and M. Dua, "Low-resolution Human Identification in thermal imagery," 2020 5th International Conference on Communication and Electronics Systems (IC- CES), Coimbatore, India, 2020, pp. 1283-1287, doi: 10.1109/ICCES48766.2020.9138039.

[7] Na, Xin & Yang, J. & Shuoyu, Wang. (2018). Path tracking control of an indoor transportation robot utilising future information of the desired trajectory. International Journal of Innovative Computing, Information and Control. 14. 561-572.

[8] Hindustan Times:”Siachen:How harsh is weather of world’s highest battlefield?”Hindustan Times, April 10,2024