Improvising Authorization with color-based ID card detection

PHASE 1 REPORT

Submitted by

HARINI MURUGAN [201501013],

NIKITHA K R [201501031],

RAGAVI M [201501038]

in partial fulfillment for the award of the degree of

BACHELOR OF TECHNOLOGY IN ARTIFICIAL INTELLIGENCE AND MACHINE LEARNING

RAJALAKSHMI ENGINEERING COLLEGE

ANNA UNIVERSITY : CHENNAI 600 025

NOVEMBER, 2023

ANNA UNIVERSITY : CHENNAI 600 025

BONAFIDE CERTIFICATE

Certified that this project report "**IMPROVISING AUTHORIZATION WITH COLOR-BASED ID CARD DETECTION**" is the bonafide work of "**Harini Murugan (201501013), Nikitha K R(201501031), Ragavi M (201501038)** " who carried out the project work under my supervision. Certified further that to the best of my knowledge the work reported herein does not form part of any other project report or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE	**SIGNATURE**
Dr. N. Srinivasan	Mrs.S.Mahalakshmi
HEAD OF THE DEPARTMENT	**SUPERVISOR**
B.Tech Artificial Intelligence	B.Tech Artificial Intelligence
and Machine Learning	and Machine Learning
Rajalakshmi Engineering College	Rajalakshmi Engineering College
Chennai – 602 105	Chennai – 602 105

This project report is submitted for Project Viva-Voce Examination held on ____________ .

INTERNAL EXAMINER **EXTERNAL EXAMINER**

ACKNOWLEDGEMENT

Initially, we thank the Almighty for being with us through every walk of our life. It is our privilege to express our sincerest thanks to our respected Chairman **Mr. S. Meganathan, B.E, F.I.E.,** and beloved chairperson **Dr. (Mrs.) Thangam Meganathan, M.A., M.Phil., Ph.D** and beloved Vice Chairman **Mr. Abhay Shankar Meganathan, B.E, M.S** for providing us with the requisite infrastructure and extending support in all endeavors.

Our heartfelt thanks to **Dr. S. N. Murugesan, M.E., Ph.D.,** our Principal for his kind support and resources provided to complete our work in time. We deeply express our sincere thanks to **Dr. N. Srinivasan, Ph.D.,** Head of the Department of Artificial Intelligence and Machine Learning for his encouragement and continuous support to complete this project in time. We are glad to express our sincere thanks and regards to our supervisor, **Mrs. S. Mahalakshmi, B.E., M.E.,** Assistant Professor, Department of Artificial Intelligence and Machine Learning and to our coordinator Dr. Indira Priya, **M.E., Ph.D** Professor, Department of Artificial Intelligence and Machine Learning for their guidance and suggestion throughout the course of the project.

Finally we express our thanks for all teaching, not teaching, faculty and our parents for helping us with the necessary guidance during the time of our project.

Harini Murugan (201501013)

Nikitha K R (201501031)

Ragavi M (201501038)

ABSTRACT

The project "CHROMACARD: Improving Authorization With Color-Based ID Card Detection" introduces the concept of ChromaCard representing an automated apparatus designed for the authentication of access to a given location based on the coloration of an individual's ID card tag. In contrast to conventional systems reliant upon ID card readers, which necessitate manual interaction to present the tag to the device, our innovative robotic solution excels in seamlessly detecting tag colors even when in motion. Employing a sophisticated camera equipped with object detection capabilities, the robotic entity rigorously scrutinizes the hues of the ID tag. Subsequently, it cross-references this data with a comprehensive repository of validated ID cards authorized for entry to the specified location at the given moment. The determination of an individual's entitlement to access is thereby made, leading to one of two outcomes: should authorization be affirmed, the robotic system proceeds to assess the subsequent ID card; conversely, if access is denied, it promptly dispatches a notification to the student care administrator, who is in close proximity to the facility.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATION

ID	-	Identity Documentation
YOLOv4	-	You Only Look OnceVersion 4
RFID	-	Radio-Frequency Identification
QR	-	Quick Response
mAP	-	Mean Average Precision
IOU	-	Intersection Of Union
EM	-	Electromagnetic
VOC	-	Visual Object Classes
YOLOv8	-	You Only Look OnceVersion 8
SQL	-	Structured Query Language
HSV	-	Hue Saturation Value

CHAPTER 1

INTRODUCTION

Access control and authentication systems are fundamental to ensuring security and efficiency in various environments, such as educational institutions, corporate facilities, and government buildings. Traditional methods often require manual interaction with ID card readers, which can result in delays, congestion, and potential security vulnerabilities. In response to these challenges, our project introduces ChromaCard, an innovative robotic apparatus designed to revolutionize access authentication based on the coloration of an individual's ID card tag.

ChromaCard utilizes a sophisticated camera equipped with object detection capabilities to seamlessly and accurately detect the colors on ID card tags, even when individuals are in motion. The system cross-references this color data with a comprehensive database of validated ID cards authorized for entry to a specific location at a given moment. This rigorous scrutiny of ID tag hues and instant data analysis leads to one of two outcomes. If authorization is confirmed, the robotic system proceeds to assess the next ID card, ensuring a swift and efficient process. Conversely, if access is denied, ChromaCard promptly dispatches a notification to the nearby student care administrator, allowing for immediate response to unauthorized access attempts.

In this project report, we integrate object detection and color analysis technologies. We also discuss the significance of innovation in access control systems, the potential applications of ChromaCard in various sectors, and the pivotal role it plays in enhancing security while streamlining access control processes. The aim of this report is to provide a comprehensive understanding of how ChromaCard represents a game-changing solution for access authentication, offering improved security and operational efficiency in a wide range of environments.

1.1 Background and Significance of Access Control Systems:

Access control systems are fundamental components of security and efficiency across diverse settings, serving as a safeguard in educational institutions, corporate facilities, and beyond. These systems are designed to manage and monitor entry, ensuring that only authorized individuals gain access to specific areas. Their significance lies in safeguarding against unauthorized access, theft, and potential security breaches. Conventional manual ID card reader systems, while widely used, exhibit limitations, often causing bottlenecks and security concerns due to the need for manual interaction. Thus, there is a compelling need for innovative solutions to address these issues and enhance access control processes.

1.1.1 Historical Evolution of Access Control :

The historical evolution of access control has a remarkable transformation over time. From ancient methods like locks and keys to the digital age of biometric and card-based systems, access control has evolved in response to the changing needs of society. Early access control was rudimentary, relying on physical barriers, but the advent of electronic systems brought greater sophistication and efficiency. However, even these systems had their limitations, requiring manual card presentation. The introduction of innovative solutions like ChromaCard marks, harnessing advanced technology to provide secure, efficient, and automated access control based on color authentication, a significant step forward in the historical progression of access control systems.

1.1.2 Diverse Applications of Access Control:

Access control is not limited to one specific sector. Its significance is exemplified in education, where it tracks student attendance and enhances safety. In corporate settings, it secures valuable assets and sensitive information. Additionally, government facilities and healthcare institutions rely on access control to safeguard critical areas and sensitive data. Access control is versatile, with its importance extending to various sectors. Its adaptability demonstrates the need for solutions like ChromaCard that can address the unique requirements of each application.

1.1.3 Security and Safety Concerns:

Ensuring secure and efficient access control is essential for safeguarding individuals and assets. Inadequate access control systems can lead to breaches, unauthorized entries, theft, and even physical harm. The significance of this topic lies in emphasizing that security and safety are paramount, particularly in environments like educational institutions where the well-being of students and staff is of utmost importance. Security and safety concerns make access control systems critical. ChromaCard's innovative approach aligns with the need to enhance security and safety while streamlining access processes.

1.1.4 Limitations of Traditional Access Control Methods:

Traditional manual ID card reader systems are widely used but are not without their drawbacks. These systems can create bottlenecks, especially in high-traffic environments, leading to inefficiencies. Additionally, they rely on manual user interactions, which can introduce the potential for human error or unauthorized access, highlighting the need for more automated and reliable solutions. Recognizing the limitations of traditional methods is essential for understanding why innovative access control solutions like ChromaCard, which overcome these limitations, are significant for improving access processes.

1.1.5 The Role of Technology in Access Control Advancements:

The integration of advanced technology in access control systems has played a pivotal role in shaping the field. Innovations such as biometrics, smart cards, and automated robotic solutions like ChromaCard have pushed the boundaries of what's possible in access control, demonstrating the impact of technology on the industry. Technology has been a driving force behind the evolution of access control systems, making them more secure, efficient, and adaptable. ChromaCard's technological advancements make it a prime example of how innovation can transform access control.

1.2 The Need for Innovation in Access Control:

The demand for innovation in access control systems is a response to the limitations of traditional methods, which become particularly evident in high-traffic environments. Conventional systems relying on manual ID card readers can result in bottlenecks and operational inefficiencies. In busy places like airports, educational institutions, and major events, the manual interaction required for access verification can cause delays and congestion. Moreover, human error is always a factor, and the risk of unauthorized access looms large. Innovative solutions are needed to address these issues and enhance access control in high-traffic areas. The significance of incorporating advanced technology into access control systems cannot be overstated. Advanced technology not only streamlines the access verification process but also enhances security. Automation reduces the need for human intervention, minimizing errors and reducing the time taken for each verification. Additionally, the integration of cutting-edge technology allows for real-time data analysis and decision-making, ensuring that access is granted or denied promptly. In a world where security concerns are ever-present, leveraging technology to enhance access control is crucial in safeguarding both people and sensitive information.

1.3 Introducing ChromaCard: An Innovative Robotic Solution:

1.3.1 Introducing chromacard:

ChromaCard is a pioneering automated apparatus designed to revolutionize access authentication. It stands out as a novel solution in the realm of access control systems. This robotic entity brings automation to the forefront, eliminating the need for manual ID card presentation. It excels at detecting ID tag colors, even when individuals are in motion. By doing so, it streamlines and enhances the efficiency of access control processes, setting it apart from traditional systems.

1.3.2 Key features of ChromaCard:

It includes its innovative color-based authentication method. This allows it to identify individuals based on the colors of their ID card tags, a process that is both rapid and accurate. Real-time detection capabilities ensure that access verification is swift and secure, contributing to the system's effectiveness. ChromaCard is designed to address the limitations of traditional methods and elevate access control to a new level, where security and efficiency coexist seamlessly.

1.4 Technological Underpinnings: Object Detection and Color Analysis

1.4.1 Object detection:

The technical components of ChromaCard are at the heart of its innovation. The apparatus is equipped with a sophisticated camera that boasts object detection capabilities. This means that it can not only capture ID card data but also recognize and track moving objects, including the ID card tags themselves. This dynamic tracking capability ensures that ChromaCard can identify individuals even as they walk past the access point, which is a significant improvement over traditional static ID card readers.

1.4.2 Color analysis:

It is another critical aspect of ChromaCard's technology. The system scrutinizes the colors present on the ID card tags with precision. It cross-references this color data with a comprehensive database of validated ID cards, authorized for entry at that specific location at the given moment. This meticulous analysis ensures that the system can accurately determine the authenticity of the ID card, minimizing the risk of false positives or negatives. In summary, the combination of object detection and color analysis makes ChromaCard a highly reliable and efficient access control solution.

1.5 Authorization and Notification: ChromaCard in Action

ChromaCard plays a pivotal role in determining an individual's entitlement to access a specified location. It does so by rigorously analyzing the coloration of the individual's ID card tag and cross-referencing it with a database of validated ID cards. This real-time analysis leads to swift and accurate decisions, ensuring that only authorized individuals gain access. There are two potential outcomes of this analysis. If authorization is affirmed, ChromaCard seamlessly proceeds to assess the next ID card, maintaining a rapid and efficient process. Conversely, if access is denied due to an invalid ID card or other factors, ChromaCard promptly dispatches a notification to the nearby student care administrator. This immediate response ensures that unauthorized access attempts are addressed in real-time, enhancing security and providing a robust system for access control.

CHAPTER 2

LITERATURE

REVIEW

[1] TITLE:A Real-Time Moving Object Detection System Based on aDual-Spectrum Camera.

AUTHORS: Baoquan Shi, Weichen Gu and Xudong Sun

YEAR: 2022

This paper introduces XDMOM, an efficient and cost-effective video surveillance system for real-time moving object detection in outdoor environments. It comprises four key components: an imaging subsystem with a dual-spectrum camera and rotary platform, a power-efficient NVIDIA GeForce GT1030-based video processing unit, a portable lithium battery for flexible power supply, and an alarm system. XDMOM provides 360-degree, all-day monitoring while maintaining low power consumption (60~70 W). The system employs the YOLOv4-tiny neural network for object detection and an adaptive moving pipeline filter to reduce false alarms. Experimental results demonstrate an impressive 85.17% correct alarm rate during the day and 81.79% at night, particularly for monitoring humans in outdoor environments, showcasing its performance compared to state-of-the-art systems.

[2] TITLE: Research on the Detection and Tracking Algorithm of Moving Object in Image Based on Computer Vision Technology

AUTHORS: Chunsheng Chen and Din Li

YEAR: 2021

In this paper, an innovative moving object detection and tracking algorithm, rooted in computer vision technology, is introduced to enhance video image processing. The study conducts a comprehensive comparison of the inter frame difference method and the background difference model method, both theoretically and experimentally. Subsequently, the Robert edge detection operator is chosen for vehicle edge detection. Research findings reveal that the algorithm in this paper exhibits the longest frame processing time when tracking moving targets, approximately 2.3 times that of the CamShift algorithm. This algorithm boasts high operational efficiency, meeting real-time tracking requirements for foreground targets. It excels in tracking accuracy, reduces time consumption, and minimizes frame tracking errors compared to the actual target position.

[3] TITLE:Two Layer Security System Using RFID & Face Detection.

AUTHORS: Ashok Kumar Yadav, Ramnaresh, Kumar Abhishek, Akash Kumar, Adil Khan, Vikash Sangwan.

YEAR: 2019

In this paper, a two-layer security system is introduced, combining RFID (Radio Frequency Identification) and biometric facial detection, aimed at maximizing security in attendance marking. The system begins with RFID scanning, generating a unique card ID for a user via an RFID Reader. Following this, facial detection through a webcam is initiated to mark attendance, ensuring that only authorized individuals can register their attendance. This dual-layer security approach offers enhanced authentication, with RFID streamlining the initial step and face detection bolstering security by cross-referencing against an authorized person database. This combination of steps provides an effective and robust security solution for attendance management.

[4] TITLE: Moving Object Detection for Event-based Vision using Graph Spectral Clustering.

AUTHORS: Anindya Mondal,Shashant R, Jhony H. Giraldo,Thierry Bouwmans and Ananda S. Chowdhury.

YEAR: 2020

In this paper, the focus is on moving object detection in Neuromorphic Vision Sensors, which capture events in an asynchronous manner, mimicking the human eye's operation. While these sensors offer advantages like high dynamic range, low latency, and low power consumption, they pose challenges due to noise and low resolution in the event data. Additionally, event-based data lack typical visual information such as texture and color. To address this, the paper introduces an unsupervised Graph Spectral Clustering technique for Moving Object Detection in Event-based data. The approach also automates the determination of the optimal number of moving objects. Experimental results on publicly available datasets demonstrate that the GSCEventMOD algorithm outperforms several state-of-the-art techniques by up to 30%.

[5] TITLE: Authentication for ID Cards based on Colour Visual Cryptography and Facial Recognition.

AUTHORS: D. R. Ibrahim, R. Abdullah, J. S. Teh, B. Alsalibi.

YEAR: 2018

In this paper, the focus is on enhancing the authentication process for modern identification cards used in various applications, such as electronic passports and payment cards. The paper addresses the need for robust user authentication beyond passwords, including biometric data like fingerprints and iris images. To achieve this, a novel authentication method is proposed, combining color visual cryptography and facial recognition. The user's color image is encrypted using visual cryptography, producing two share images—one stored in the card and the other in a database. Placing the card on a sensor allows the two shares to overlap, revealing the original image. This recovered image is then processed by a trained facial recognition algorithm to verify the user's identity. The paper presents an evaluation of the method based on recognition rate and runtime, with experimental results demonstrating its practical feasibility and potential for future development in this area.

[6] TITLE: Moving Object Detection Technology of Line Dancing Based on Machine Vision.

AUTHORS: Liyun Liu.

YEAR: 2021

In this paper, the focus is on advancing moving object detection technology in the context of line dancing using machine vision. To improve object detection accuracy, the study combines an enhanced frame difference technique for background modeling with a target detection algorithm. This approach allows for the extraction of moving targets and subsequent post-morphological processing to refine the detection process. The paper also discusses the tracking of these moving targets over time, determining their positions in each frame and establishing associations between similar targets in consecutive frames. Through specific measurement criteria, the mean-shift algorithm is applied to search for the optimal candidate target in each image frame, facilitating moving object tracking. The experimental analysis demonstrates that this method can effectively detect moving targets in line dancing scenarios, unaffected by their position or distance, consistently achieving highly accurate detection results.

[7] TITLE:Automatic Toll Collection System using RFID.

AUTHORS: Sumathi S M,Nikhitha Kale M,Manasa R,Jithesh A,Megha D. Hegde.

YEAR: 2018

This paper introduces an RFID-based Automated Toll Collection System to enhance traffic management and digitalization in Bangladesh. It eliminates delays on toll roads, bridges, and tunnels by using RFID technology to identify vehicles for toll collection, without requiring cash payments or stopping vehicles. Tags attached to digital number plates are used for this purpose, reducing the need for manual ticket distribution and toll collection. The system promotes seamless information exchange between vehicle owners and toll authorities, ensuring transparency and reducing manual labor and errors, contributing to a more efficient transportation system in Bangladesh.

[8] TITLE: Student Identity Card Based On Advanced Quick Response Code Technology.

AUTHORS: Saheed Y.K. & Salau-Ibrahim T.T.,Kadri A. F..

YEAR: 2016

In this paper, the focus is on enhancing the means of student identification in Al-Hikmah University by introducing a Quick Response code student identity card to replace the existing student ID card. The proposed system employs QR codes generated from a virtual server, containing links to individual student records. By scanning the QR code on the student's ID card, the system can access the database and retrieve the student's academic information. This innovative approach not only improves data integrity and confidentiality but also establishes a unique and efficient method for identifying Al-Hikmah University students.

[9] TITLE: Object Detection Based on Deep Learning and B-Spline Level Set in Color Images.

AUTHORS: Lin Zhang, Xinyu Zhang, Ning An , Rui Gao, and Yingjie Zhang.

YEAR: 2022

This paper focuses on object detection using deep learning techniques, covering both object recognition and precise three-dimensional positioning. The method comprises three components: object recognition and coarse positioning via deep learning, precise positioning using deep learning with B-spline level set in color images, and achieving accurate three-dimensional positioning with depth information from an RGB-D camera. These precise object positioning techniques provide vital end pose data for autonomous robotic arm grasping, significantly impacting robotic manipulation. Performance metrics include mAP and IOU . Experimental results demonstrate Yolo-v3 achieving an mAP of

87.62% and an average IOU of 66.74%. Additionally, combining Yolo-v3 with B-spline level set results in a 100% average IOU, ensuring accurate 3D object localization in real-world scenarios. Comparisons with VOC dataset results highlight the superiority of the proposed dataset in terms of mAP and average IOU values.

[10] TITLE: A High Bandwidth End-Effector with Active Force Control for Robotic Polishing.

AUTHORS: Jian Li, Yisheng Guan, Haowen Chen, Bing Wang, Tao Zhang, Xineng Liu, Jie Hong, Danwei Wang.

YEAR: 2021

This study focuses on using a neural network model to classify RFID tags based on their EM signatures, primarily for authentication in chipless RFID technology to combat counterfeiting. EM characteristics provide unique, unclonable fingerprints that enhance security. The study involves 18 V band (65-72 GHz) tags, known for their sensitivity to dimensional variations, ideal for highlighting EM signature differences. Machine learning is used to characterize and classify these EM responses, achieving a maximum recognition rate of 100%, surpassing related RFID fingerprinting works in accuracy. The study employs a random search algorithm to determine the optimal network configuration and compares different learning algorithms to fine-tune the system in terms of accuracy and loss.

CHAPTER 3
SYSTEM OVERVIEW

3.1 EXISTING SYSTEM:

3.1.1 CURRENT EXISTING SYSTEMS:

The following are the existing system that resemble our proposed system - “Improvising Authorization with color-based ID card detection” :

Proximity Card Systems: Proximity card systems use contactless smart cards or RFID cards. Users simply need to bring their cards close to a card reader to gain access.Proximity card systems are also known as proximity key cards or proximity access cards, for authentication and authorization purposes. These systems are widely used in various environments to control access to secure areas and provide an efficient and convenient means of entry.

Barcode or QR Code Scanners: Barcode and QR code scanners are devices or software applications designed to read and decode barcodes and QR codes for various purposes. They are commonly used in retail, inventory management, logistics, ticketing, marketing, and many other applications.

Smart Card Systems: Smart card systems are secure and versatile technologies that use integrated circuit chips to store and manage data. These cards, often resembling credit card-sized plastic cards, have found wide-ranging applications in various industries, from access control and payment systems to identification and secure data storage.

Biometric Authentication:

Biometric authentication is a security process that uses an individual's unique physiological or behavioral characteristics to verify their identity. This technology has gained widespread use in various applications, including access control, personal devices, and identity verification.

3.1.2 DRAWBACKS OF THE EXISTING SYSTEM :

There are many errors and complications faced in these existing systems and even area for developments present the systems:

Proximity cards can be duplicated if an attacker gains access to the card or the data stored on it. This can happen through cloning the card or stealing the card's data.

Proximity cards need to be very close to the card reader for authentication, typically within a few inches or centimeters. This can be less convenient than contactless smart cards, which have a greater range.

Barcode and QR code scanners are generally considered less secure than some other authentication methods, such as biometrics. They rely on the knowledge of the code rather than the inherent uniqueness of the individual. Anyone with a copy of the code can potentially gain access

Issuing and replacing smart cards can be administratively complex and costly. If a card is lost or damaged, it needs to be replaced, which can be a time-consuming process.

Smart cards have limited storage capacity compared to other data storage devices. This can restrict the amount of data that can be stored on the card, which may be a limitation for some applications.

Environmental Factors play a vital role in Biometric authentication - Lighting conditions: Poor or uneven lighting can affect the accuracy of facial recognition and iris scanning,environmental noise: Background noise can impact voice recognition accuracy and temperature and humidity: Fingerprint recognition can be influenced by temperature and humidity, leading to false rejections.

3.2 PROPOSED SYSTEM:

3.2.1 BASE PROPOSED SYSTEM :

Our proposed robot works to identify the unauthorized students in the canteen areas around the campus through their ID card tag color. In contrast to conventional systems reliant upon ID card readers, which necessitate manual interaction to present the tag to the device, our innovative robotic solution excels in seamlessly detecting tag colors even when in motion.Our robot consists of a camera that uses object detection to analyze the color of the ID tag.The robot can then compare this information to a database of known valid ID cards that can access that particular location at that time and decides if the individual is authorized to be there or not.The determination of an individual's entitlement to access is thereby made, leading to one of two outcomes: should authorization be affirmed, the robotic system proceeds to assess the subsequent ID card; conversely, if access is denied, it promptly dispatches a notification to the student care administrator, who is in close proximity to the facility.

3.2.2 SYSTEM COMPONENTS:

Our Proposed System components involve:

Robot with Camera:

The system includes a mobile robot equipped with a camera capable of capturing images of ID card tags.

ID Card Tags:

Students and authorized individuals are provided with ID card tags with color-coding, signifying their access permissions.

Object Detection Algorithm:

The robot's camera is integrated with an object detection algorithm to identify and analyze the color of the ID card tags.

Database of Authorized ID Cards:

The system maintains a database of authorized ID cards and their corresponding access permissions. This database is regularly updated to reflect changes in access rights.

Student Care Administrator Interface:

The student care administrator has access to a dedicated interface or mobile application that provides real-time notifications and access control features.

3.2.3 PROPOSED SYSTEM BENEFITS:

The proposed system holds a variety of benefits such as:

Real-time Detection: The system can identify unauthorized students in real time as the robot moves through the canteen area.

Automated Authentication: Unlike manual ID card readers, this system does not require manual presentation of ID cards, making it seamless and efficient.

Enhanced Security: By automating the access control process, the system reduces the risk of human error and improves overall security on campus.

Immediate Notifications: The system promptly alerts the student care administrator in the event of an access denial, allowing for immediate action.

Scalability: The system can be scaled to cover multiple areas on campus, offering a comprehensive access control solution.

Data Logging: The system can maintain a log of access attempts and outcomes for auditing and reporting purposes.

3.3 FEASIBILITY STUDY:

A feasibility study for our proposed system involves assessing the practicality, viability, and potential benefits of implementing such a system. Here are the main components to consider in a feasibility study for this project:

Project Scope and Objectives:

- Clearly define the project's scope and objectives. Determine what specific areas or access points you intend to secure using color-based ID card detection.

Technical Feasibility:

- Evaluate the technical aspects of implementing the system:
  - Assess the availability of the necessary technology, such as ID card tags, RFID readers, cameras, and object detection algorithms.
  - Determine if the infrastructure can support real-time processing and decision-making.
  - Investigate the availability of suitable hardware and software components.

Resource Requirements:

- Identify the resources needed for the project, including hardware, software, personnel, and funding. Consider factors such as maintenance, updates, and technical support.

Data Security and Privacy:

- Examine the data security and privacy implications of the system:
  - Assess the security measures in place to protect biometric data and access control data.
  - Ensure compliance with data protection laws and regulations.

Cost Analysis:

- Conduct a cost-benefit analysis to determine the financial feasibility of the project:
  - Estimate the initial implementation costs, including hardware, software, and setup.
  - Evaluate ongoing operational and maintenance costs.
  - Compare the costs to the potential benefits, including enhanced security and efficiency.

Legal and Regulatory Compliance:

- Ensure that the project complies with all relevant laws and regulations, including data privacy and security requirements.

User Acceptance:

- Assess the willingness of users, such as students and staff, to adopt the system:
  - Consider conducting surveys or gathering feedback to gauge user acceptance.
  - Address concerns and communicate the benefits of the system to users.

Environmental and Physical Considerations:

- Evaluate environmental factors and the physical conditions in which the system will operate:
  - Ensure that lighting conditions are suitable for accurate color detection.
  - Consider factors like temperature, humidity, and possible obstacles in the environment.

Risk Assessment:

- Identify potential risks and challenges that may impact the project's success. Develop mitigation strategies to address these risks.

Scalability:

- Consider whether the system can be easily scaled to accommodate a larger user base or additional access points.

Alternative Solutions:

- Explore alternative security solutions, such as other biometric methods, access control technologies, or combination approaches, and assess their feasibility.

Timeline and Implementation Plan:

- Create a timeline for the project, including key milestones and deadlines. Develop an implementation plan outlining the sequence of activities.

Conclusion and Recommendation:

- Based on the assessment of technical, financial, legal, and user-related factors, conclude the feasibility study with a recommendation. Determine whether to proceed with the project, make adjustments, or reconsider the implementation.

CHAPTER 4
SYSTEM REQUIREMENTS

4.1 Hardware Requirements

4.1.1 Computer:

Operating system: Windows 10 or Linux

CPU: Intel Core i5 or AMD Ryzen 5 or higher

Memory: 8 GB RAM or more

Storage: 128 GB SSD or more

4.1.2 Camera:

High-resolution camera with object detection capabilities

Supported camera models:

Intel RealSense D435i

Nvidia Jetson Nano Developer Kit

Google Coral Dev Board

Raspberry Pi 4 with a USB camera

4.2 Software Requirements

4.2.1 Programming languages:

Python 3.7 or higher

4.2.2 Libraries and frameworks:

OpenCV

TensorFlow

PyTorch

Flask or Django (optional for the notification system)

4.2.3 Database:

MySQL, PostgreSQL, or a cloud-based database service such as Amazon Aurora or Google Cloud SQL

CHAPTER 5

SYSTEM DESIGN

5.1 SYSTEM ARCHITECTURE DIAGRAM:

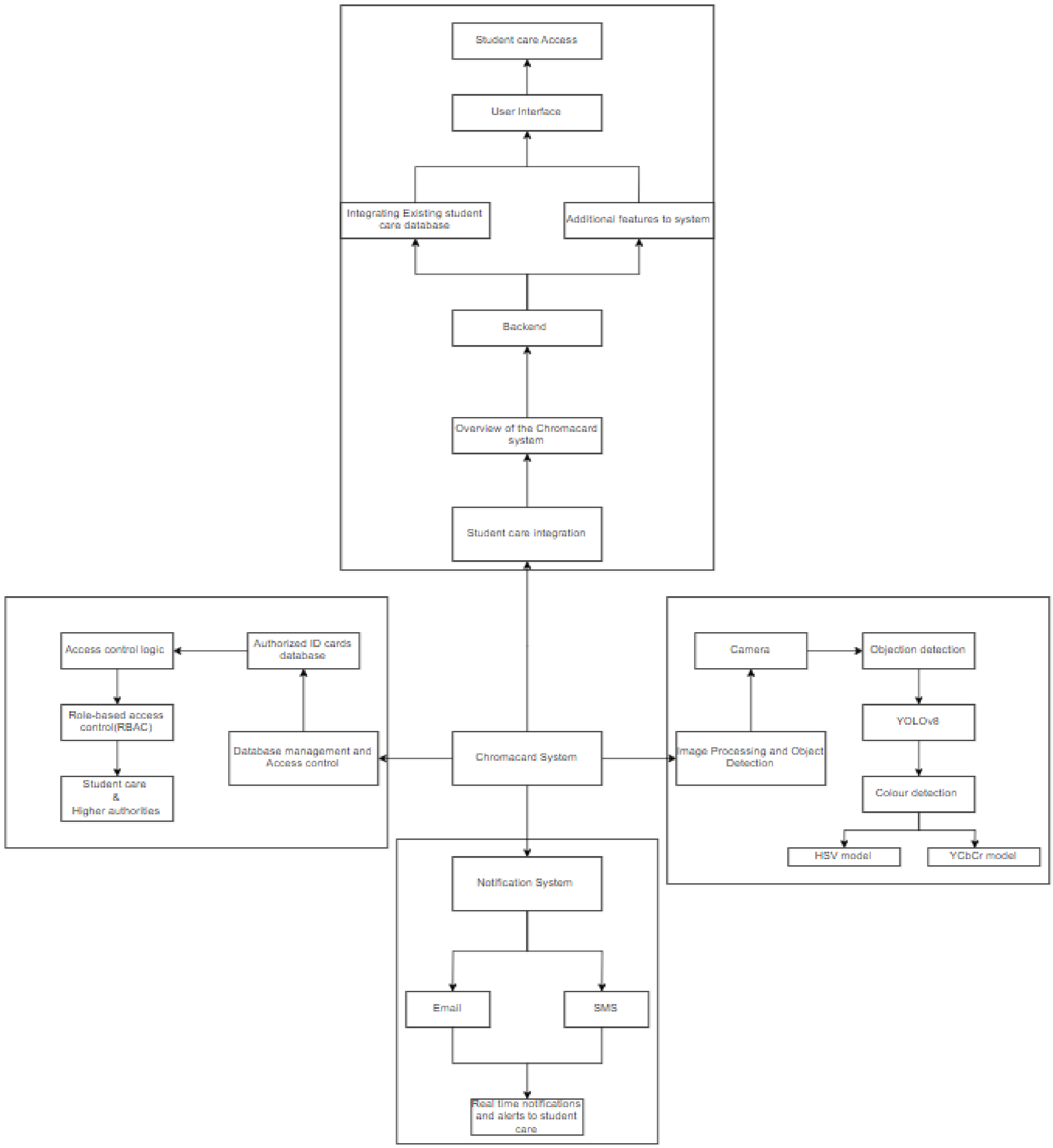


Figure 5.1 System Architecture diagram

5.2 MODULE DESCRIPTION:

5.2.1 MODULE 1: Image Processing and Object Detection

Objectives:

The Image Processing and Object Detection module plays a crucial role in the proposed system for improving authorization with color-based ID card detection. This module is responsible for capturing, processing, and analyzing images of ID card tags in real-time to determine whether an individual is authorized to access a particular area. Develop an image processing module to capture and analyze the color of ID card tags.

Object Detection: YOLO V8

Algorithm Description: YOLO v8 is a real-time object detection system that excels in recognizing multiple objects within a single image or frame. It divides an image into a grid, where each grid cell predicts the presence of various objects and their associated bounding boxes. YOLO v8 uses deep convolutional neural networks to make predictions efficiently and accurately.

Role in Object Recognition: YOLO v8 enhances the system's ability to identify and locate objects amidst clutter, thanks to its speed and accuracy. It's particularly useful in real-time applications where rapid object recognition is essential.

Object detection with YOLO involves the following steps:

Input Image or Video Stream: YOLO takes an input image or a video stream as its input.

Image Preprocessing: The input image is preprocessed, which may involve resizing, normalization, and other transformations to prepare it for object detection.

Neural Network Architecture: YOLO utilizes a convolutional neural network (CNN) as its core architecture. The specific architecture may vary with different YOLO versions, but they are typically designed for real-time object detection.

Feature Extraction: The neural network extracts features from the input image at different scales and levels, capturing information at multiple resolutions. This enables YOLO to detect objects of various sizes in the image.

Bounding Box Prediction: YOLO divides the image into a grid of cells and predicts bounding boxes around objects within each cell. These bounding boxes include information about the object's location (center coordinates), width, height, and a confidence score.

Object Class Prediction: For each bounding box, YOLO also predicts the probability distribution over multiple object classes, indicating what the detected object is (e.g., car, person, dog).

Non-Maximum Suppression (NMS): After predictions are made for all grid cells, YOLO performs non-maximum suppression to eliminate duplicate or highly overlapping bounding boxes and retain the most confident predictions.

Output Results: YOLO provides the final list of detected objects along with their class labels and bounding box coordinates. These results can be displayed on the image or used for further processing.

Colour Detection: HSV and YCbCr color model - Both the HSV and YCbCr color models offer advantages in color detection tasks. HSV is particularly useful for specifying colors based on human perception, while YCbCr can be effective in separating chromatic information from luminance. The choice between these models depends on the specific requirements of the color detection task.

Tasks:

- Configure the camera to capture high-quality images.
- Implement image processing algorithms to isolate and identify ID card tags.
- Extract and store the color information from the detected ID tags.

DFD FOR MODULE 1:

The data flow diagram of this module shows a diagram of the steps involved in ID card detection and color matching:

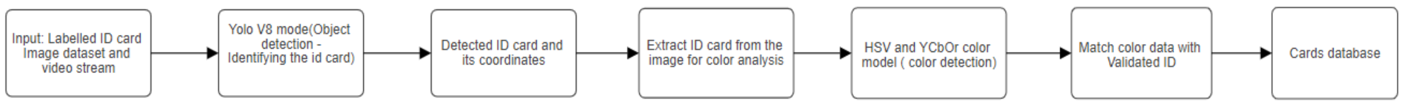


Figure 5.2 DFD 1

1. Input: The input to the system is a labeled ID card image dataset and video stream.

2. YOLO V8 mode: The first step is to use YOLO V8 to detect the ID card in the image or video frame. YOLO V8 is a state-of-the-art object detection model that can detect multiple objects in real time.

3. Detected ID card and its coordinates: Once the ID card has been detected, the system extracts the ID card from the image or video frame and its coordinates.

4. Extract ID card from the image for color analysis: The extracted ID card is then analyzed to determine its color. This can be done using a color space such as HSV or YCbCr.

5. HSV and YCbCr color model (color detection): The HSV and YCbCr color models are both well-suited for color detection. The HSV color model is perceptually uniform, meaning that colors that are close together in the HSV color space are also perceived as being close together. The YCbCr color model is more robust to changes in illumination and contrast.

6. Match color data with Validated ID Cards database: The color data of the extracted ID card is then matched with a database of validated ID cards. This database contains the color data of all valid ID cards issued by a particular government or organization.

7. Output: The output of the system is a decision of whether the ID card is valid or not.

5.2.2 MODULE 2: Database Management and Access Control

Objectives:

To Establish a Database for ID Card Information and Implementing Access Control Logic. To create a Database and to establish a structured database that serves as a repository for information regarding valid ID cards and authorized access. This database will play a crucial role in managing access to specific locations or resources. It develops access control logic that evaluates an individual's ID card to determine if they are authorized to access a particular location at a given time. This logic is fundamental in ensuring security and authorization within the system.

Database Schema Design:

ID Card Information: This table stores data related to ID cards, such as card ID, cardholder details, and color information.

Access Permissions: Specify access rules, encompassing authorized locations, timeframes, and individuals.

Database Operations Module Development:

Adding Records: Create functions or procedures for adding new records to the database. This is necessary for incorporating new valid ID cards or modifying access rules.

Updating Records: Implement features for updating existing records, enabling changes to card information, access permissions, or timestamps.

Deleting Records: Develop procedures for deleting records from the database, especially when ID cards become invalid or access permissions are revoked.

Access Control Logic Implementation:

Authorization Rules: Define criteria and rules for assessing individuals' authorization, considering factors like ID card validity, specified access timeframes, and other conditions.

Decision-Making: Develop logic that evaluates authorization rules when an access request is made. The system will then decide whether to grant or deny access based on the assessment.

Integration with ID Card Detection: Ensure seamless integration with Module 1 (Image Processing and Object Detection). The results of object detection will be used in conjunction with the access control logic to make access decisions.

Logging and Auditing:

Access Event Logging: Implement mechanisms to log access events in the database, recording details such as who accessed specific locations, when the access occurred, and the conditions under which it happened.

Auditing: Enable auditing features to review access history and identify any unauthorized access attempts or unusual patterns.

Tasks:

- Design a database schema to store ID card color information, associated access permissions, and timestamps.

- Develop a module for adding, updating, and deleting records in the database.
- Implement access control logic to determine if an individual's ID card is authorized to access the location at a given time.

DFD FOR MODULE 2:

The data flow diagram of this module shows a diagram of the steps involved in ID card detection and color matching:

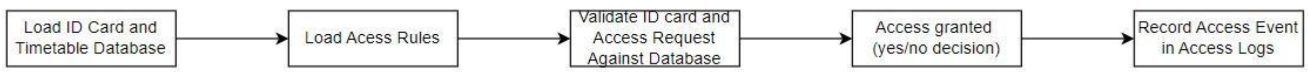


Figure 5.3 DFD 2

1) Load ID Card and Timetable Database: It loads data from the ID card database and the timetable database. These databases contain information about individuals and their schedules.

2) Load Access Rules: Its access rules specify who is allowed to access certain areas or resources. It could include information on which individuals are authorized to access specific areas or at certain times.

3) Validate ID Card and Access Request Against Database: The system verifies the validity of the Vardale ID card and the access request against the loaded databases. It checks if the person's identity and access request comply with the access rules.

4) Access Granted (Yes/No Decision): Based on the comparison of the Vardale ID card, access request, and access rules, the system makes a decision whether to

grant or deny access. If the person's request complies with the rules, access is granted (Yes), otherwise, it is denied (No).

5) Record Access Event in Access Logs: If access is granted, the system records this access event in access logs. Access logs are essential for tracking who accessed what, when, and where. They serve security and auditing purposes.

CHAPTER 6

CONCLUSION AND FUTURE ENHANCEMENT

6.1 CONCLUSION:

In conclusion, the ChromaCard project has culminated in the development of a sophisticated and dependable access control and authentication system that promises to have a transformative impact on security and user convenience. The innovative techniques, including color-based authentication, motion detection, advanced camera technology, data cross-referencing, and immediate notification, has forged a system that excels in surpassing the limitations of traditional ID card reader systems.

ChromaCard's strengths are multifaceted. Firstly, its color-based authentication mechanism not only enhances security but also offers a more intuitive and user-friendly means of access control. This innovative approach eliminates the need for manual interactions with card readers and provides seamless detection of tag colors, even when individuals are in motion.

The incorporation of motion detection adds an additional layer of security, ensuring that the system remains vigilant and responsive to dynamic scenarios. Advanced camera technology facilitates clear and accurate image capture, while the ability to process these images in real-time sets the system apart, minimizing waiting times and optimizing user experience.

Furthermore, the system's capacity to cross-reference color data with a comprehensive database of authorized ID cards ensures that access control decisions are made with precision and accuracy. This feature not only enhances security but also simplifies the management of access permissions.

The real-time notification system is another hallmark of ChromaCard. Its ability to promptly alert relevant personnel, such as student care administrators, in the event of access denials or security breaches enhances the overall security infrastructure.

6.2 FUTURE ENHANCEMENT:

The ChromaCard project is already an innovative and advanced access control and authentication system. However, there are several potential areas for future enhancement and development to further improve its capabilities and versatility:

1. Biometric Integration: Integrating biometric authentication methods, such as facial recognition or fingerprint scanning, can enhance security and provide an additional layer of identity verification.

2. Machine Learning and AI: Leveraging machine learning and artificial intelligence can improve the system's object detection capabilities and enable it to learn and adapt to new object types and scenarios over time.

3. Mobile Application: Developing a mobile application that allows users to access and manage their permissions, receive notifications, and interact with the system remotely can enhance user convenience.

4. User Analytics: Collecting and analyzing user data can provide insights into user behavior and help optimize the system's performance and user experience.

APPENDIX:

A1.1 SAMPLE CODE

CODE FOR OBJECT DETECTION:

```
import cv2
from flask import Flask, render_template, request, redirect, Response, send_from_directory
from ultralytics import YOLO

app = Flask(_name_)
# Placeholder for the password (you can implement a more secure solution)
PASSWORD = "1234"

# OpenCV VideoCapture object to access the camera
camera = cv2.VideoCapture(0)  # Use '0' for the default camera, change to other numbers for different cameras if available

def generate_frames():
    model = YOLO("yolov8s.pt")
    while True:
        success, frame = camera.read()
        if not success:
            break
        else:
            # Convert the frame to JPEG format
            result = model.predict(frame)
            for box in result[0].boxes.xyxy.tolist():
                cv2.rectangle(frame, (int(box[0]), int(box[1])), (int(box[2]), int(box[3])), (0, 255, 0),
            ret, buffer = cv2.imencode('.jpg', frame)
            frame = buffer.tobytes()
```

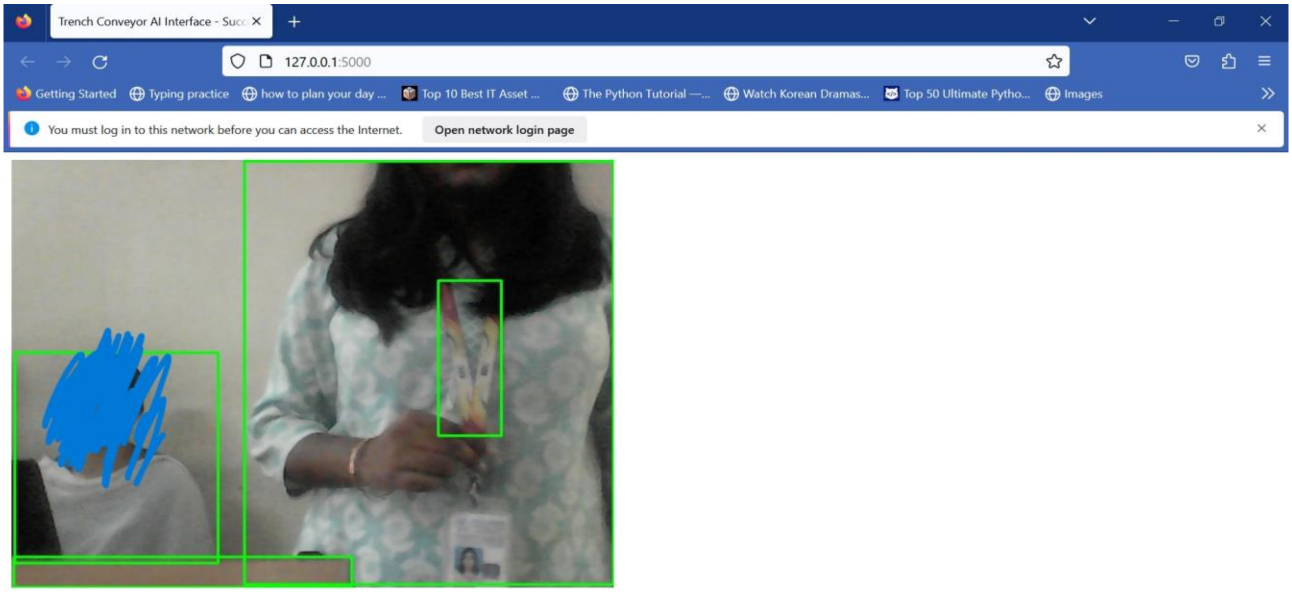
```
        yield (b'--frame\r\n'
               b'Content-Type: image/jpeg\r\n\r\n' + frame + b'\r\n')


@app.route("/", methods=["GET", "POST"])
def home():
    return render_template("home.html")


@app.route('/video_feed')
def video_feed():
    return Response(generate_frames(), mimetype='multipart/x-mixed-replace; boundary=frame')


if _name_ == "_main_":
    app.run(debug=True)
```

```
<!DOCTYPE html>
<html>
<head>
    <title>Trench Conveyor AI Interface - Successful</title>


<body>
    <!-- <div class="container-video"> -->
        <!-- <div class="logo logo-left"><img src="{{ url_for('static', filename='assets/REC Logo.png') }}" width="200px" height="auto"></div> -->
        <!-- <div class="logo logo-right"><img src="{{ url_for('static', filename='assets/Apollo logo.png') }}" width="160px" height="auto"></div> -->
        <!-- <h1 class="title">Trench Conveyor AI Interface</h1> -->
            <!-- <div class="sub-containers-wrapper"> -->
                <!-- <h4>Feed 1 and 2</h4> -->
```

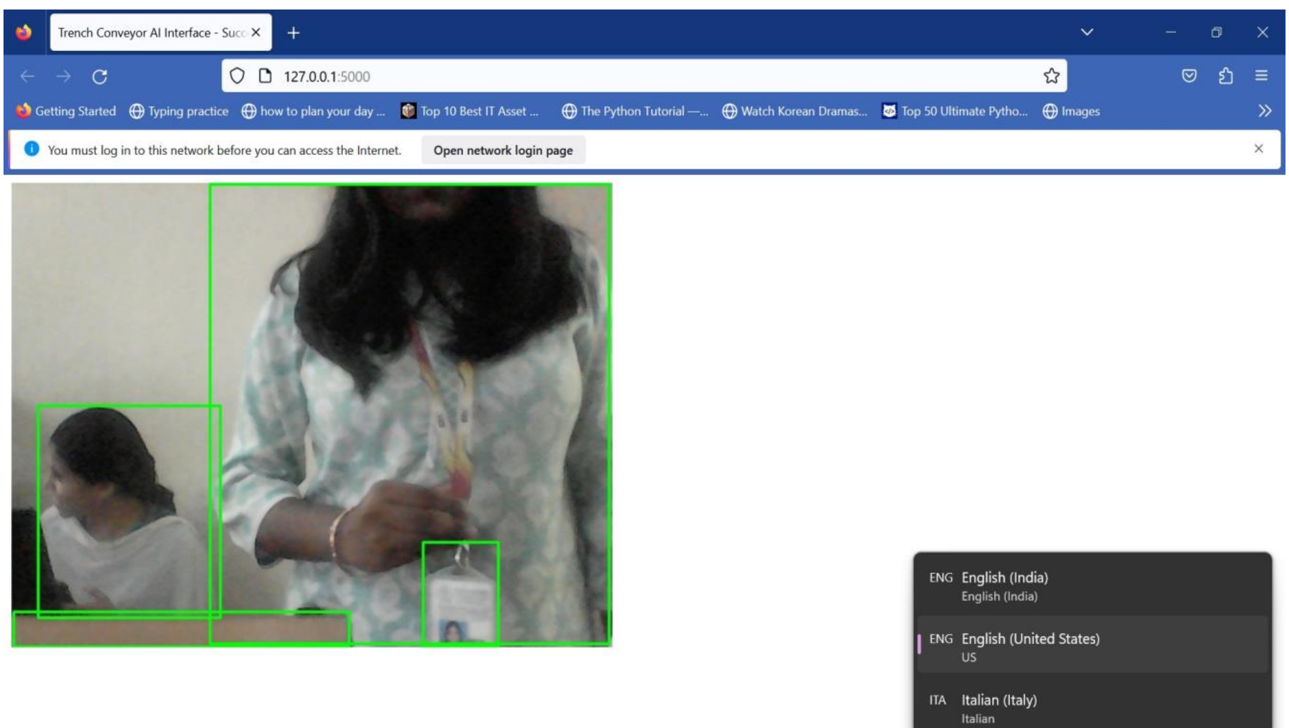
```
            <!-- <div class="sub-container-video"> -->
              <img  id="video-player" class="video-player" width="600" height="auto" controls src="{{ url_for('video_feed') }}" alt="Camera Feed">
                  

              <!-- <img  id="video-player" class="video-player" width="600" height="auto" controls src="{{ url_for('video_feed') }}" alt="Camera Feed"> -->
            <!-- </div> -->
            <!-- <h4>Feed 3 and 4</h4> -->
            <!-- <div class="sub-container-video">
              <img  id="video-player" class="video-player" width="600" height="auto" controls src="{{ url_for('video_feed') }}" alt="Camera Feed">
                  
              <img  id="video-player" class="video-player" width="600" height="auto" controls src="{{ url_for('video_feed') }}" alt="Camera Feed">
            </div> -->
          <!-- </div> -->
          <script>
            // Get all video player elements
            const videoPlayers = document.querySelectorAll('.video-player');

            // Attach click event listeners to each video player
            videoPlayers.forEach(player => {
              player.addEventListener('click', (event) => {
                event.stopPropagation(); // Prevent the click from propagating to the document
                videoPlayers.forEach(otherPlayer => {
                  if (otherPlayer !== player) {
                    otherPlayer.classList.remove('enlarged');
                  }
```

```
                });
                player.classList.toggle('enlarged');
            });
        });

        // Attach a click event listener to the document
        document.addEventListener('click', () => {
            videoPlayers.forEach(player => {
                player.classList.remove('enlarged');
            });
        });
    </script>
        <script src="{{ url_for('static', filename='js/script_three.js') }}"></script>
  </div>
</body>
```

A1.2 SCREENSHOTS



SCREENSHOT: TAG DETECTED



SCREENSHOT: ID CARD DETECTED

REFERENCES

[1] Baoquan Shi, Weichen Gu and Xudong Sun (2022) 'A Real-Time Moving Object Detection System Based on a Dual-Spectrum Camera'.

[2] Chunsheng Chen and Din Li (2021) 'Research on the Detection and Tracking Algorithm of Moving Objects in Image Based on Computer Vision Technology'.

[3] Ashok Kumar Yadav, Ramnaresh, Kumar Abhishek, Akash Kumar, Adil Khan, Vikash Sangwan (2019) 'Two Layer Security System Using RFID & Face Detection'.

[4] Anindya Mondal,Shashant R, Jhony H. Giraldo,Thierry Bouwmans and Ananda S. Chowdhury (2020) 'Moving Object Detection for Event-based Vision using Graph Spectral Clustering'.

[5] D. R. Ibrahim, R. Abdullah, J. S. Teh, B. Alsalibi (2018) 'Authentication for ID Cards based on Colour Visual Cryptography and Facial Recognition,' Robotics and Computer-Integrated Manufacturing'.

[6] Liyun Liu (2021) 'Moving Object Detection Technology of Line Dancing Based on Machine Vision'.

[7] Sumathi S M,Nikhitha Kale M,Manasa R,Jithesh A,Megha D. Hegde (2018) 'Automatic Toll Collection System using RFID'.

[8] Saheed Y.K. & Salau-Ibrahim T.T.,Kadri A. F. (2016) 'Student Identity Card Based On Advanced Quick Response Code Technology'.

[9] Lin Zhang, Xinyu Zhang, Ning An , Rui Gao, and Yingjie Zhang (2022) 'Object Detection Based on Deep Learning and B-Spline Level Set in Color Images'

[10]Dragos, Nastasiu , Razvan Scripcaru (2019) 'A New Method of Secure Authentication Based on Electromagnetic Signatures of Chipless RFID Tags and Machine Learning Approaches'.

LIST OF PUBLICATIONS

S. NO.	NAME OF THE CONFERENCE	APPLIED DATE	ACCEPTANCE / REJECTION STATUS
1.	WILEY Online Library	15/11/2023	On Process
2.	Scope journal of Educational and social Research	15/11/2023	On Process