KSCST

Karnataka State Council for Science and Technology

(An autonomous organisation under the Dept. of Science & Technology, Govt. of Karnataka)
Indian Institute of Science Campus, Bengaluru – 560 012
Telephone: 080-23341652, 23348848, 23348849, 23348840
Email: office.kscst@iisc.ac.in, office@kscst.org.in • **Website:** www.kscst.iisc.ernet.in, www.kscst.org.in

Dr. U T Vijay
Executive Secretary

19th April, 2024

Ref: 7.1.01/SPP/37

To,
The Principal
Alva's Institute of Engineering and Technology
Shobavana Campus Mijar
Moodbidri - 574 225

Dear Sir/Madam,

Sub : Sanction of Student Project - 47th Series: Year 2023-2024

Project Proposal Reference No. : **47S_BE_1729**
Ref : Project Proposal entitled **VISITOR FACE AUTHENTICATION DESIGN USING OPEN CV**

We are pleased to inform that your student project proposal referred above, has been approved by the Council under "Student Project Programme - 47th Series". The project details are as below:

Student(s)	Ms. LIKHITA K. M.	**Department**	INFORMATION SCIENCE AND ENGINEERING
	Mr. RAVINDRA REDDY		
	Mr.SHASHANK BIRADAR		
	Mr. SURAJ S. ANKOLEKAR	**Sanctioned Amount (in Rs.)**	4,500.00
Guide(s)	Dr. PRADEEP V.		

Instructions:

a) The project should be performed based on the objectives of the proposal submitted.

b) Any changes in the project title,objectives or students team is liable for rejection of the project and your institution shall return the sanctioned funds to KSCST.

c) Please quote your project reference number printed above in all your future correspondences.

d) After completing the project, 2 to 3 page write-up (synopsis) needs to be uploaded on to the following Google Forms link https://forms.gle/6s8hq5XbScsBMv3G9. The synopsis should include following:

1) Project Reference Number
2) Title of the project
3) Name of the College & Department
4) Name of the students & Guide(s)
5) Keywords
6) Introduction / background (with specific reference to the project, work done earlier, etc) - about 20 lines
7) Objectives (about 10 lines)

8) Methodology (about 20 lines on materials, methods, details of work carried out, including drawings, diagrams etc)

9) Results and Conclusions (about 20 lines with specific reference to work carried out)

10) Scope for future work (about 20 lines).

e) In case of incompeted projects, the sanctioned amount shall be returned to KSCST.

f) The sanctioned amount will be transferred by NEFT to the bank account provided by the College/Institute.

g) The sponsored projects evaluation will be held **third week of May 2024** onwards through Online Mode and the details of the same will be intimated shortly by email / Website

h) After completion of the project, soft copy of the project report duly signed by the Principal, the HoD, Guide(s) and studetn(s) shall be uploaded in the following Google Forms Link https://forms.gle/Mi446v1U5fdFcMD99. The report should be prepared in the format prescribed by the university.

i) The **Utilization Certificate and Statement of Expenditure duly signed by competent authority** of consolidated sanctioned projects from your institution need to be submitted **20 August 2024** without fail.

Please visit our website for further announcements / information and for any clarifications please email to spp@kscst.org.in

Thanking you and with best regards,

Yours sincerely,

Vijay

(U T Vijay)

Copy to:

1) The HoD
INFORMATION SCIENCE AND ENGINEERING
ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY, MOODBIDRI

2) Dr. PRADEEP V.
INFORMATION SCIENCE AND ENGINEERING
ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY, MOODBIDRI

3) THE ACCOUNTS OFFICER
KSCST, BENGALURU

PRINCIPAL
Alva's Institute of Engg. & Technology,
Mijar. MOODBIDRI - 574 225, D.K

VISVESVARAYA TECHNOLOGICAL UNIVERSITY
BELGAUM, KARNATAKA- 590014

A PROJECT REPORT ON

VISITOR FACE AUTHENTICATION USING OPEN-CV

Submitted in partial fulfillment for the award of Degree of,

BACHELOR OF ENGINEERING

IN

INFORMATION SCIENCE AND ENGINEERING

By

LIKHITA K M	4AL20IS021
RAVINDRA REDDY	4AL20IS039
SHASHANK BIRADAR	4AL20IS044
SURAJ ANKOLEKAR	4AL20IS052

Under the guidance of

Dr. PRADEEP V

Associate Professor

DEPARTMENT OF INFORMATION SCIENCE AND ENGINEERING

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY
MIJAR, MOODBIDRI D.K -574225

2023-24

ALVA'S INSTITUTE OF ENGINEERING AND TECHNOLOGY

MIJAR, MOODBIDRI D.K. -574225

KARNATAKA

ALVA'S

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

CERTIFICATE

This is to certify that the project entitled **"VISITOR FACE AUTHENTICATION USING OPEN-CV"** has been successfully completed by

LIKHITA K M	**4AL20IS021**
RAVINDRA REDDY	**4AL20IS039**
SHASHANK BIRADAR	**4AL20IS044**
SURAJ ANKOLEKAR	**4AL20IS052**

the bonafide students OF **DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING, Alva's Institute of Engineering and Technology**, Moodbidri affiliated to **VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI** during the academic year 2023–24. It is certified that all corrections/suggestions indicated for Internal Assessment have been incorporated in the report deposited in the departmental library. The project report has been approved as it satisfies the academic requirements in respect of project work prescribed in partial fulfillment of awarding Bachelor of Engineering degree.

Dr. Pradeep V **Associate Professor** **Project Guide**	**Dr. Sudheer Shetty** **Professor** **HOD ISE**	**Dr. Peter Fernandes** **Principal**

H. O. D.
Dept. Of Information Science & Engineering
Alva's Institute of Engg. & Technology
Mijar, MOODBIDRI - 574 225

PRINCIPAL
Alva's Institute of Engg. & Technology,
Mijar, MOODBIDRI - 574 225, D.K

Name of the Examiners	**Signature with Date**
1. Dr Sudheer Shetty	30/5/24
2. Dr. Ritesh Paurala	Apaurala 30/05/24

ALVA'S INSTITUTE OF ENGINEERING & TECHNOLOGY MIJAR, MOODBIDRI D.K. -574225 KARNATAKA

DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING

DECLARATION

LIKHITA K M	**4AL20IS021**
RAVINDRA REDDY	**4AL20IS039**
SHASHANK BIRADAR	**4AL20IS044**
SURAJ ANKOLEKAR	**4AL20IS052**

hereby declare that the dissertation entitled, **"VISITOR FACE AUTHENTICATION USING OPEN- CV"** is completed and written by us under the supervision of our guide **Dr. Pradeep V, Associate Professor, Department of Information Science and Engineering, Alva's Institute of Engineering And Technology, Moodbidri,** in partial fulfillment of the requirements for the award of the degree BACHELOR OF ENGINEERING in **DEPARTMENT OF INFORMATION SCIENCE & ENGINEERING** of the **VISVESVARAYA TECHNOLOGICAL UNIVERSITY, BELAGAVI** during the academic year 2023-24. The project report is original and it has not been submitted for any other degree in any university.

LIKHITA K M	4AL20IS021
RAVINDRA REDDY	4AL20IS039
SHASHANK BIRADAR	4AL20IS044
SURAJ ANKOLEKAR	4AL20IS052

ACKNOWLEDGEMENT

The satisfaction and euphoria that accompany a successful completion of any task would be incomplete without the mention of people who made it possible, success is the epitome of hard work and perseverance, but steadfast of all is encouraging guidance.

So, with gratitude we acknowledge all those whose guidance and encouragement served as beacon of light and crowned the effort with success.

We thank our beloved Principal **Dr. PETER FERNANDES,** for his constant help and support throughout.

We sincerely thank, **Dr. SUDHEER SHETTY**, Professor and Head, Department of Information Science & Engineering who has been the constant driving force behind the completion of the project.

The selection of this Synopsis as well as the timely completion is mainly due to the interest and persuasion of our Project guide **Dr. PRADEEP V,** Associate Professor, Department of Information Science & Engineering. We will remember his contribution for ever.

We thank our beloved Project Coordinator **Prof. JAYANTKUMAR A RATHOD,** Associate Professor, Department of Information Science & Engineering, for his constant guidanceand help.

We are indebted to **Management of Alva's Institute of Engineering and Technology, Mijar, Moodbidri** for providing an environment which helped us in completing our Synopsis.

LIKHITA K M	4AL20IS021
RAVINDRA REDDY	4AL20IS039
SHASHANK BIRADAR	4AL20IS044
SURAJ ANKOLEKAR	4AL20IS052

ABSTRACT

we introduce an advanced visitor face authentication system that integrates OpenCV, deep learning, and the YOLOv4 algorithm to enhance security and streamline the verification process in various settings such as offices, residential buildings, and secure facilities. The system employs YOLOv4 for precise and efficient face detection, ensuring real-time performance even in dynamic and crowded environments. For authenticating visitors, we use a deep learning model trained on an extensive dataset of facial images, providing high accuracy and reliability. OpenCV is utilized for image preprocessing, feature extraction, and implementing the deep learning model. The system captures a visitor's facial image, detects the face using YOLOv4, and matches it against a database of authorized individuals. Our design is scalable and adaptable, effectively handling different lighting conditions and environmental challenges. The system also features continuous learning capabilities, allowing it to improve over time with new data. Experimental results show the system's effectiveness in terms of detection speed, accuracy, and robustness, demonstrating its potential as a practical solution for face authentication in real-world applications.

INDEX

LIST OF FIGURES

LIST OF TABLES

INTRODUCTION

CHAPTER 1

INTRODUCTION

In an era where security concerns are paramount, the development of effective visitor face authentication systems is crucial for safeguarding sensitive areas and information. Visitor authentication systems serve as the frontline defense, ensuring that only authorized individuals are granted access to restricted premises or resources. Traditional methods of authentication, such as keycards or passwords, are susceptible to theft, loss, or unauthorized duplication, highlighting the need for more robust and reliable solutions.

The advent of computer vision technologies has revolutionized the field of security, offering sophisticated tools for facial recognition and authentication. Among these technologies, OpenCV (Open Source Computer Vision Library) stands out as a versatile and widely used platform for developing computer vision applications. Its extensive collection of algorithms and functionalities make it an ideal choice for tasks such as face detection and recognition.

The research proposes a novel approach to visitor face authentication by harnessing the capabilities of OpenCV in tandem with Histogram of Oriented Gradients (HOG) features. The utilization of OpenCV facilitates accurate and efficient face detection, while HOG features enable the extraction of discriminative facial characteristics essential for authentication. By integrating these technologies into a unified system, The research aims to enhance the security measures of various establishments, ranging from corporate offices to government facilities.

1.1 PROBLEM STATEMENT

Visitor authentication systems are pivotal for ensuring secure access to restricted areas, yet existing methods face challenges. Traditional authentication means like keycards lack reliability and are prone to breaches. Current facial recognition systems, although promising, encounter issues in accuracy, real-time performance, integration complexity, and privacy concerns. Achieving accurate and efficient visitor authentication amidst varying conditions remains a challenge. Integrating OpenCV and Histogram of Oriented Gradients (HOG) for facial recognition introduces complexities in system cohesion and data privacy. Overcoming these hurdles is critical for developing a robust visitor face authentication system that balances security, efficiency, and privacy. The research aims to address these challenges, leveraging OpenCV and HOG features to create a reliable and effective visitor authentication solution for diverse security environments.

1.2 OBJECTIVES

- Enhance Accuracy: Improve the precision of visitor authentication by refining face detection and recognition algorithms to effectively identify individuals under diverse conditions.

- Optimize Real-time Performance: Streamline processing capabilities to ensure rapid authentication responses, minimizing delays and latency issues in high-traffic security environments.

- Simplify Integration: Develop seamless integration strategies for OpenCV and HOG features, reducing complexities in system cohesion and facilitating straightforward deployment.
- Address Privacy Concerns: Implement robust encryption and data protection mechanisms to safeguard facial data, ensuring compliance with privacy regulations and mitigating risks of unauthorized access.

- Ensure Scalability: Design the authentication system to accommodate varying user loads and adapt to evolving security requirements without compromising performance or accuracy.

- User-Friendly Interface: Create an intuitive user interface for system administrators and operators, facilitating easy configuration, monitoring, and management of the authentication system.

- Validation and Testing: Conduct extensive validation and testing procedures to evaluate the system's performance, accuracy, and reliability across a range of real-world scenarios and environments**.**

1.3 SYSTEM ANALYSIS

- Requirements Gathering: Conduct a comprehensive analysis of user requirements, security specifications, and environmental factors to determine the functional and non-functional requirements of the visitor face authentication system.

- Feasibility Study: Evaluate the technical feasibility of integrating OpenCV and HOG features for visitor authentication, considering factors such as computational resources, compatibility with existing infrastructure, and potential constraints.

- Risk Assessment: Identify potential risks and challenges associated with system implementation, including algorithmic limitations, data privacy concerns, integration complexities, and scalability issues. Develop mitigation strategies to address these risks effectively.

- Performance Evaluation: Perform benchmarking tests and simulations to assess the performance of the authentication system in terms of accuracy, speed, resource utilization, and scalability under various operating conditions.

- Usability Analysis: Conduct usability studies and user feedback sessions to evaluate the user interface design, system usability, and overall user experience. Incorporate feedback to enhance system usability and optimize user interaction with the authentication system.

- Resource Assessment: Assess the computational resources, hardware, and software requirements necessary for implementing the authentication system, ensuring adequate provisioning for optimal performance.

LITERATURE SURVEY

CHAPTER 2

LITERATURE SURVEY

2.1 SCOPE OF LITERATURE SURVEY

Overview of Plant Diseases: This section may provide an overview of common plant diseases and their causes, symptoms, and effects on crops. It may also discuss traditional methods of detecting and treating plant diseases.

Image Processing Techniques: This section may discuss various image processing techniques used in leaf disease detection, such as segmentation, feature extraction, and image enhancement.

Convolutional Neural Networks: This section may provide an overview of Convolutional Neural Networks (CNNs) and their architecture. It may also discuss various techniques for optimizing and fine-tuning CNNs for leaf disease detection.

Applications and Case Studies: This section may review real-world applications of leaf disease detection using CNNs and provide case studies of successful implementations.

2.2 LITERATURE SURVEY

[1]. Real-time Face Recognition and Tracking for Secure Visitor Access Control using OpenCV and Deep Learning

Author: T.A. Tran, T.L. Nguyen, X.H. Pham (2020)

The paper combines OpenCV and deep learning for real-time face recognition and tracking to bolster visitor access control. However, the integration of deep learning increases system complexity and processing demands. Additionally, real-time tracking raises privacy concerns. Thorough analysis is required to evaluate resource requirements, performance, and privacy considerations. Mitigation strategies may include optimizing algorithms for efficiency, implementing privacy-enhancing measures such as data anonymization, and ensuring user consent. Balancing enhanced security with usability and privacy is crucial for the system's effectiveness.

[2]. Title: Lightweight Deep Learning Model for Efficient Visitor Face Authentication on Edge Devices

Authors: S. Sharma, K.R. Geetha, N. Kannan (2022)

The paper introduces a lightweight deep learning approach for visitor face authentication on edge devices, leveraging MobileNetV2 for feature extraction. This model balances accuracy with computational efficiency, crucial for edge devices with limited resources. While promising, there are potential drawbacks to consider. MobileNetV2 may yield lower accuracy compared to more complex models, necessitating careful evaluation against performance requirements. Additionally, specific hardware optimizations may be required to ensure optimal performance on edge devices. Thorough system analysis is necessary to assess resource constraints, performance metrics, and potential risks associated with lower accuracy. Mitigation strategies may include exploring hardware optimization techniques and conducting extensive performance testing to validate the model's effectiveness under real-world conditions. Overall, balancing efficiency and accuracy is key to the success of visitor face authentication on edge devices, ensuring reliable security measures while optimizing resource utilization.

[3].Edge AI-powered Visitor Face Authentication System with Attention-based Deep Learning

Authors: M. Singh, V. Sharma, P. Gupta (2023)

The paper introduces an Edge AI-powered Visitor Face Authentication System, merging OpenCV for face detection with an attention-based deep learning model to enhance accuracy and resource utilization on edge devices. This approach aims to streamline visitor authentication while minimizing computational overhead. However, deployment on specific edge hardware necessitates careful optimization, potentially posing challenges in adapting to diverse hardware configurations. Furthermore, constraints on model size and complexity may limit the system's scalability and adaptability to varying use cases. Therefore, thorough system analysis is crucial to assess hardware compatibility, performance metrics, and potential limitations associated with model size and complexity. Mitigation strategies may include targeted hardware optimizations and model compression techniques to ensure efficient deployment and reliable performance in edge environments. Balancing accuracy with hardware constraints is essential for the system's effectiveness and widespread adoption in real-world applications.

[4]. Title: Federated Learning for Collaborative Visitor Face Authentication in Decentralized Settings

Authors: L. Sun, Z. Li, Y. Fang (2023)

The paper presents a novel approach to collaborative visitor face authentication in decentralized settings, leveraging federated learning across multiple sites. The system utilizes OpenCV for local face detection, ensuring privacy by processing data locally without sharing sensitive information. However, while federated learning enables model training without centralizing data, it introduces increased communication overhead due to frequent model updates across distributed nodes. Additionally, privacy and security concerns arise from the decentralized nature of the system, necessitating robust encryption and authentication protocols to safeguard sensitive data during communication. Moreover, ensuring compliance with privacy regulations and addressing potential vulnerabilities in federated learning protocols are essential challenges. Thorough analysis and implementation of privacy-preserving techniques, along with stringent security measures, are imperative to mitigate these drawbacks and ensure the effectiveness and trustworthiness of the collaborative visitor face authentication system in decentralized environments.

[5]. Multi-Camera Facial Authentication for Accurate Visitor Matching in Complex Environments

Authors: W. Jiang, M. Yuan, Y. Huang (2021)

Recent advancements in multi-camera facial authentication have focused on mitigating drawbacks while enhancing system performance. One notable improvement is the integration of edge computing capabilities to alleviate processing demands associated with managing multiple cameras. By deploying edge devices near camera clusters, preprocessing tasks such as face detection and tracking can be distributed, reducing the burden on centralized servers. Additionally, advancements in computer vision algorithms, particularly in deep learning-based methods, have led to more robust and accurate face detection and tracking across multiple cameras. Techniques such as feature fusion and attention mechanisms have been employed to improve the matching accuracy of visitor authentication systems in complex environments. Furthermore, advancements in hardware technology, such as high-resolution sensors and low-power processing units, have enabled more efficient and cost-effective deployment of multi-camera facial authentication systems in diverse settings.

[6]. Title: Liveness Detection for Secure Visitor Authentication using OpenCV and Liveness Tests

Authors: M.M. Rahman, M.S.U. Rahman, M.A. Hossain (2020)

The paper presents an innovative approach to secure visitor authentication by integrating liveness detection techniques with OpenCV. By incorporating measures such as eye blinking and head movement detection, the system aims to thwart spoofing attempts and enhance security before proceeding with facial recognition. However, the inclusion of liveness detection introduces additional steps in the authentication process, potentially extending the overall processing time and user experience. Moreover, certain liveness tests, such as infrared imaging for blood flow detection, may require specialized hardware, increasing implementation costs and infrastructure complexity. Despite these drawbacks, the integration of liveness detection with OpenCV represents a significant advancement in combating biometric spoofing attacks and ensuring the integrity of visitor authentication systems. Further research and development efforts may focus on optimizing liveness detection algorithms and minimizing hardware dependencies to enhance the practicality and scalability of the proposed approach.

[7]. Title: Liveness Detection for Secure Visitor Authentication using OpenCV and Liveness Tests Approach

Authors: M.M. Rahman, M.S.U. Rahman, M.A. Hossain (2020)

The paper proposes an integration of liveness detection with OpenCV to bolster security in visitor authentication. By employing techniques like eye blinking and head movement analysis, the system aims to counter spoofing attempts prior to facial recognition. However, the incorporation of liveness tests introduces extra steps in the authentication process, potentially prolonging overall processing time and user experience. Furthermore, specific liveness tests may necessitate specialized hardware, increasing implementation costs and complexity. Despite these drawbacks, this approach signifies a significant stride in combating biometric spoofing attacks and ensuring the integrity of authentication systems. Future research could concentrate on refining liveness detection algorithms to minimize processing overhead and exploring alternative methods that mitigate hardware dependencies, thereby optimizing the practicality and scalability of the proposed solution.

[8]. Title: Real-time Face Recognition and Tracking for Secure Visitor Access Control using OpenCV and Deep Learning

Authors: T.A. Tran, T.L. Nguyen, X.H. Pham (2020)

The paper introduces a system for secure visitor access control that integrates OpenCV and deep learning. By combining face detection, real-time tracking, and deep learning-based, the system aims to enhance security measures. However, this integration introduces increased complexity and processing demands, potentially impacting system performance. Furthermore, real-time tracking raises privacy concerns, as it involves continuous monitoring of individuals' movements. The tracking aspect of the system may lead to potential privacy breaches if not implemented with appropriate safeguards. Despite these drawbacks, the proposed system represents a significant advancement in visitor access control, offering improved security through real-time face recognition and tracking. Future research could focus on mitigating privacy concerns through the implementation of robust privacy protection mechanisms and optimizing system performance to address the increased processing demands.

[9]. Title: Hybrid Deep Learning and OpenCV Approach for Enhanced Visitor Face Authentication

Authors: S. Das, S. Kumar, P.L.N. Raju (2019)

The paper proposes a hybrid approach for visitor face authentication, amalgamating deep learning and OpenCV techniques. It leverages a pre-trained VGG16 network for feature extraction and Principal Component Analysis (PCA) for dimensionality reduction, enhancing the accuracy of authentication. OpenCV is employed for face detection and preprocessing, streamlining the initial stages of the authentication process. However, the hybrid approach demands substantial computational resources due to the utilization of deep learning models and complex algorithms, potentially posing challenges for deployment on resource-constrained systems. Additionally, the integration of multiple technologies may introduce implementation complexities, requiring specialized expertise for system setup and configuration. Despite these drawbacks, the hybrid approach represents a significant advancement in visitor face authentication, offering improved accuracy and robustness. Future research efforts could focus on optimizing computational efficiency and simplifying implementation procedures to facilitate broader adoption of the proposed approach in real-world security applications.

[10]. Title: Privacy-Preserving Visitor Authentication using Local Differential Privacy with OpenCV

Authors: Y. Zhang, Z. Wang, M. Li (2018)

The paper introduces a privacy-preserving approach for visitor authentication, employing Local Differential Privacy (LDP) in conjunction with OpenCV. By integrating LDP, the system aims to safeguard visitor facial data while still maintaining acceptable recognition accuracy levels. However, the implementation of LDP may entail a potential trade-off between privacy and accuracy, as the anonymization process could introduce noise that affects recognition performance. Moreover, integrating LDP with OpenCV increases computational complexity, as additional steps are required to ensure privacy protection without sacrificing system efficiency. Despite these drawbacks, the proposed approach represents a significant advancement in addressing privacy concerns associated with visitor authentication systems. Future research may focus on optimizing the balance between privacy and accuracy, as well as developing more efficient algorithms for LDP integration to minimize computational overhead and facilitate widespread adoption of privacy-preserving authentication techniques.

[11]. Development of a Real Time Emotion Recognition System Using Facial Expressions and EEG based on machine learning and deep neural network methods (2020).

Author: Aya Hassouneh, A.M. Mutawa, M. Murugappan

The study highlights the importance of automatic emotion recognition in healthcare and smart technologies. Emphasizing the challenges in recognizing emotions, the paper discusses the growing role of AI and machine learning in pattern recognition, focusing on human computer interaction. The study proposes a real-time system using virtual markers on facial expressions and EEG signals, with a methodology involving marker placement, tracking via the Lucas Kande algorithm, and feature extraction for machine learning classifiers. The innovation lies in reduced computational complexity, addressing challenges faced by offline systems. Objectives include real-time recognition of six basic emotions, benefiting physically disabled individuals and children with Autism. Evaluation metrics involve mean emotional recognition rate, specificity, and sensitivity. The research contributes to emotion recognition with potential applications in healthcare and personalized e-learning.

[12]. Human Facial Emotion Detection Using Deep Learning (2022)

Author: Dharma Karan Reddy Gaddam, Mohd Dilshad Ansari, Sandeep Vuppala, Vinit Kumar Gunjan, and Madan Mohan Sat

The paper proposes a deep learning model for facial emotion recognition using ResNet50 and demonstrates its effectiveness on the FER2013 dataset. The model outperforms other networks, achieving a test accuracy of 55.6%. The emphasize the significance of deep learning, particularly CNNs, in addressing the complexities of emotion recognition. They highlight the importance of the convolutional layer, pooling layer, and fully connected layer in CNNs and discuss the addition of a dropout layer to prevent overfitting. The study contributes to the field of facial emotion recognition.

[13]. Optimal Speed and Accuracy of Object Detection (2020)

Author: Alexey Bochkovskiy, Chien-Yao Wang, Hong-Yuan Mark Liao.

Optimal Speed and Accuracy of Object Detection" presents an enhanced version of the popular object detection algorithm YOLO (You Only Look Once). Authored by Alexey Bochkovskiy, Chien-Yao Wang, and Hong-Yuan Mark Liao, it introduces YOLOv4, which achieves significant improvements in both speed and accuracy compared to previous versions. YOLOv4 incorporates various architectural enhancements, training strategies, and data augmentation techniques to achieve state-of-the-art performance on object detection tasks. The authors meticulously optimize the model for real-time inference while maintaining high accuracy, making it suitable for various applications requiring fast and precise object detection, such as autonomous driving, surveillance, and robotics. This paper serves as a valuable resource for researchers and practitioners seeking advanced solutions in the field of computer vision and deep learning.

[14].On-device Face Authentication System for ATMs and Privacy Preservation (2023)

Author: A. Boragule, K. C. Yow, M. Jeon.

"On-device Face Authentication System for ATMs and Privacy Preservation" discusses the development of a face authentication system designed for ATMs, with a focus on privacy preservation. Authored by A. Boragule, K. C. Yow, and M. Jeon, the paper presents an innovative approach to face authentication that operates directly on the ATM device, eliminating the need for external servers and ensuring data privacy. The system utilizes advanced face detection and recognition techniques to authenticate users securely and efficiently. By processing facial data locally, the system minimizes the risk of privacy breaches associated with cloud-based authentication systems. This paper provides valuable insights into the design and implementation of on-device face authentication systems, offering a practical solution for enhancing security and privacy in ATM transactions.

[15]. FA-GAN: Face Augmentation GAN for Deformation-Invariant Face Recognition (2021)

Authors: M. Luo, J. Cao, X. Ma, X. Zhang, R.

"FA-GAN: Face Augmentation GAN for Deformation-Invariant Face Recognition" presents a novel approach to face recognition using Generative Adversarial Networks (GANs) for face augmentation. Authored by M. Luo, J. Cao, X. Ma, X. Zhang, and R. He, the paper introduces FA-GAN, a GAN-based framework designed to generate deformation-invariant face images. FA-GAN addresses challenges in face recognition posed by facial deformations, such as expression changes and occlusions, by generating augmented face images that are invariant to such deformations. The paper demonstrates the effectiveness of FA-GAN in improving the robustness of face recognition systems against variations in facial appearance. This research contributes to advancements in the field of face recognition by introducing a novel technique for augmenting face images to enhance recognition performance in challenging scenarios.

[16].Masked Face Recognition Using Deep Learning: A Review" (2021)

Authors: A. Alzu‘bi, F. Albalas, T. AL-Hadhrami, L.B. Younis, A. Bashayreh

"Masked Face Recognition Using Deep Learning: A Review" provides an overview of masked face recognition techniques employing deep learning. Authored by A. Alzu‘bi, F. Albalas, T. AL-Hadhrami, L.B. Younis, and A. Bashayreh, the paper examines the challenges and advancements in recognizing faces obscured by masks, particularly in the context of the COVID-19 pandemic. The review discusses various deep learning approaches and algorithms proposed for masked face recognition, highlighting their strengths, limitations, and potential applications. This comprehensive review serves as a valuable resource for researchers and practitioners interested in understanding and developing masked face recognition systems using deep learning techniques.

[17].R. He, X. Wu, Z. Sun, and T. Tan, "Learning Invariant Deep Representation for NIR-VIS Face Recognition," in Proc. 31st AAAI Conf. Artif. Intell, 2017, pp. 2020- 2021.

Authors: R. He, X. Wu, Z. Sun, T. Tan

"Learning Invariant Deep Representation for NIR-VIS Face Recognition" presents a method for learning invariant deep representations for near-infrared (NIR) and visible (VIS) face recognition. Authored by R. He, X. Wu, Z. Sun, and T. Tan, the paper proposes a deep learning approach to address the challenges of recognizing faces captured under different modalities (NIR and VIS). The proposed method learns deep representations that are invariant to modality-specific variations, thereby improving the performance of face recognition across different imaging modalities. This research contributes to advancements in face recognition technology by introducing a novel approach to learning invariant representations for NIR-VIS face recognition.

[18]. X. Di, B. S. Riggan, S. Hu, N. Short, and V. Patel, "Polarimetric thermal to visible face verification via self-attention guided synthesis," in Proc. Int. Conf. Biometrics, 2019, pp. 1–8.

Authors: X. Di, B. S. Riggan, S. Hu, N. Short, V. Patel

"Polarimetric thermal to visible face verification via self-attention guided synthesis" presents a method for verifying faces captured in polarimetric thermal images against visible face images using self-attention guided synthesis. Authored by X. Di, B. S. Riggan, S. Hu, N. Short, and V. Patel, the paper introduces a novel approach to cross-modal face verification that leverages polarimetric thermal and visible images. The proposed method employs self-attention guided synthesis to align and compare features between different modalities, improving the accuracy of face verification. This research contributes to advancements in face verification technology by addressing the challenges of verifying faces captured in different imaging modalities.

[19].K. Yu, G. Tang, W. Chen, S. Hu, Y. Li and H. Gong, "Mobile Net-YOLO v5s: An Improved Lightweight Method for Real-Time Detection of Sugarcane Stem Nodes in Complex Natural Environments," in IEEE Access, vol. 11, pp. 104070-104083, 2023, doi: 10.1109/ACCESS.2023.3317951.

Authors: K. Yu, G. Tang, W. Chen, S. Hu, Y. Li, H. Gong

"MobileNet-YOLO v5s: An Improved Lightweight Method for Real-Time Detection of Sugarcane Stem Nodes in Complex Natural Environments" presents an improved lightweight method for real-time detection of sugarcane stem nodes in complex natural environments. Authored by K. Yu, G. Tang, W. Chen, S. Hu, Y. Li, and H. Gong, the paper introduces Mobile Net-YOLO v5s, a lightweight variant of the YOLO (You Only Look Once) algorithm optimized for detecting sugarcane stem nodes. The proposed method achieves real-time performance while maintaining high accuracy in detecting stem nodes in complex natural environments. This research contributes to advancements in agricultural technology by providing an efficient and accurate method for detecting sugarcane stem nodes in field conditions.

[20].L. L. Chambino, J. S. Silva, and A. Bernardino, "Multispectral facial recognition: A review," IEEE Access, vol. 8, pp. 207871–207883, 2020, doi: 10.1109/ACCESS.2020.3037451.

Authors: L. L. Chambino, J. S. Silva, A. Bernardino

"Multispectral facial recognition: A review" provides a comprehensive review of multispectral facial recognition techniques. Authored by L. L. Chambino, J. S. Silva, and A. Bernardino, the paper examines the use of multispectral imaging for improving the accuracy and robustness of facial recognition systems. The review discusses various multispectral imaging modalities and their applications in facial recognition, highlighting their strengths, limitations, and potential research directions. This paper serves as a valuable resource for researchers and practitioners interested in understanding and implementing multispectral facial recognition technology.

[21].K. Kim, B. Lee, and J. W. Kim, "Feasibility of deep learning algorithms for binary classification problems," J. Intell. Inf. Syst., vol. 23, no. 1, pp. 95–108, Mar. 2017, doi: 10.13088/jiis.2017.23.1.095.

Authors: K. Kim, B. Lee, J. W. Kim

"Feasibility of deep learning algorithms for binary classification problems" investigates the feasibility of deep learning algorithms for binary classification problems. Authored by K. Kim, B. Lee, and J. W. Kim, the paper evaluates the performance of various deep learning algorithms on binary classification tasks and compares them with traditional machine learning methods. The study demonstrates the effectiveness of deep learning algorithms in handling binary classification problems, particularly in scenarios with complex data and nonlinear relationships. This research contributes to advancements in machine learning by providing insights into the feasibility and effectiveness of deep learning algorithms for binary classification tasks.

[22]. A. Kumari Sirivarshitha, K. Sravani, K. S. Priya, V. Bhavani, "An approach for Face Detection and Face Recognition using OpenCV and Face Recognition Libraries in Python," in 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 1274-1278, doi: 10.1109/ICACCS57279.2023.10113066.

Authors: A. Kumari Sirivarshitha, K. Sravani, K. S. Priya, V. Bhavani

An approach for Face Detection and Face Recognition using OpenCV and Face Recognition Libraries in Python" presents a method for face detection and recognition utilizing OpenCV and face recognition libraries in Python. This paper, authored by A. Kumari Sirivarshitha, K. Sravani, K. S. Priya, and V. Bhavani, describes an approach for detecting and recognizing faces in images using the OpenCV library along with face recognition libraries in Python.

[23]. S. Ren, K. He, R. Girshick, J. Sun, "Faster R-CNN: Towards real-time object detection with region proposal networks," IEEE Trans. Pattern Anal. Mach. Intell., vol. 39, no. 6, pp. 1137–1149, Jun. 2016.

Authors: S. Ren, K. He, R. Girshick, J. Sun

"Faster R-CNN: Towards real-time object detection with region proposal networks" presents the Faster R-CNN algorithm, which aims to achieve real-time object detection by integrating region proposal networks into the framework. Authored by S. Ren, K. He, R. Girshick, and J. Sun, this paper published in IEEE Transactions on Pattern Analysis and Machine Intelligence provides a detailed description of the Faster R-CNN architecture and its components The authors provide details of the algorithm and its optimization techniques, along with experimental results demonstrating its effectiveness in real-world scenarios. This research contributes to the field of computer vision by extending the applicability of real-time object detection algorithms to non-GPU computing environments.

[24]. P. Mary Jenifer, P. Mahasri, A. Omsai, B. I. Humaira, R. Dhnaalakshmi, "Multiple Face Detection and Attendance System Using OpenCV," in 2021 International Conference on Simulation, Automation & Smart Manufacturing (SASM), Mathura, India, 2021, pp. 1-5, doi: 10.1109/SASM51857.2021.9841223.

Authors: P. Mary Jenifer, P. Mahasri, A. Omsai, B. I. Humaira, R. Dhnaalakshmi

Multiple face detection and attendance tracking using OpenCV. Authored by P. Mary Jenifer, P. Mahasri, A. Omsai, B. I. Humaira, and R. Dhnaalakshmi, this paper describes the design and implementation of a face detection and attendance system using the OpenCV library. The system detects multiple faces in images captured by a camera and records attendance based on recognized faces. The authors present the methodology, system architecture, and experimental results from the implementation. This research contributes to the field of computer vision and attendance tracking systems by providing a practical solution for automated face detection and attendance recording using OpenCV.

[25]. W. Fang, L. Wang, P. Ren, "Tinier YOLO: A real-time object detection method for constrained environments," IEEE Access, vol. 8, pp. 1935–1944, 2020, doi: 10.1109/ACCESS.2019.2961959.

Authors: W. Fang, L. Wang, P. Ren

"Tinier YOLO: A real-time object detection method for constrained environments" presents a method for real-time object detection in constrained environments. Authored by W. Fang, L. Wang, and P. Ren, the paper introduces Tinier YOLO, a variant of the YOLO (You Only Look Once) object detection algorithm optimized for real-time performance in resource-constrained environments.

[26]. K. M. Lee, H. Song, J. W. Kim, C. H. Lin, "Balanced performance for efficient small object detection YOLOv3-tiny," in Proc. Korean Soc. Broadcast Eng. Conf., Anseong, South Korea: The Korean Institute of Broadcast and Media Engineers, Nov. 2018, pp. 117–118.

Authors: K. M. Lee, H. Song, J. W. Kim, C. H. Lin

"Balanced performance for efficient small object detection YOLOv3-tiny" presents a method for efficient small object detection using YOLOv3-tiny. Authored by K. M. Lee, H. Song, J. W. Kim, and C. H. Lin, the paper discusses the challenges of detecting small objects and proposes a balanced performance approach to enhance the efficiency of YOLOv3-tiny for such tasks. The authors present experimental results demonstrating the effectiveness of their approach in achieving improved performance for small object detection while maintaining computational efficiency. This research contributes to the field of object detection by addressing the specific challenges associated with detecting small objects in real-world scenarios.

[27]. J. Pedoeem, R. Huang, C. Chen, "YOLO-LITE: A real-time object detection algorithm optimized for non-GPU computers," in 2018 IEEE International Conference on Big Data (Big Data), Seattle, WA, USA, 2018, pp. 2503-2510.

Authors: J. Pedoeem, R. Huang, C. Chen

"YOLO-LITE: A real-time object detection algorithm optimized for non-GPU computers" introduces YOLO-LITE, an optimized real-time object detection algorithm designed for non-GPU computers. Presented by J. Pedoeem, R. Huang, and C. Chen at the 2018 IEEE International Conference on Big Data, the paper addresses the computational constraints of non-GPU systems and proposes YOLO-LITE as a solution for achieving real-time object detection on such platforms. The authors provide details of the algorithm and its optimization techniques, along with experimental results demonstrating its effectiveness in real-world scenarios. This research contributes to the field of computer vision by extending the applicability of real-time object detection algorithms to non-GPU computing environments.

[28]. A. Howard, M. Sandler, B. Chen, W. Wang, et al., "Searching for MobileNetV3," in 2019 IEEE/CVF International Conference on Computer Vision (ICCV), Seoul, Korea(South), 2019, pp. 1314-1324.

Authors: A. Howard, M. Sandler, B. Chen, W. Wang, et al.

"Searching for MobileNetV3" presents the search for MobileNetV3, a neural network architecture designed for efficient mobile vision applications. Presented at the 2019 IEEE/CVF International Conference on Computer Vision, the paper discusses the process of searching for an optimal neural network architecture tailored for mobile devices. The authors explore various design choices and optimization strategies to improve efficiency without compromising performance. Through extensive experiments and evaluations, they identify MobileNetV3 as a promising candidate architecture for mobile vision tasks. This research platforms, facilitating the deployment of deep learning on resource-constrained devices.

[29] K. Wang, C. Chen, Y. He, "Research on pig face recognition model based on keras convolutional neural network," in Proceeding of the 2nd International Conference on Environmental Prevention and Pollution Control Technologies (EPPCT2020), Sanya, Hainan, China, 2020, pp. 411-420.

Authors: K. Wang, C. Chen, Y. He

"Research on pig face recognition model based on keras convolutional neural network" explores the development of a pig face recognition model using the Keras convolutional neural network framework. Presented at the 2nd International Conference on Environmental Prevention and Pollution Control Technologies, the paper investigates the feasibility and effectiveness of using deep learning techniques for pig face recognition. The authors provide details of the algorithm and its optimization techniques, along with experimental results demonstrating its effectiveness in real-world scenarios. This research contributes to the field of computer vision by extending the applicability of real-time object detection algorithms to non-GPU computing environments.

[30]. M. Alsawwaf, Z. Chaczko, M. Kulbacki, N. Sarathy, "In your face: Person identification through ratios and distances between facial features," in Vietnam J. Comput. Sci., vol. 9, no. 2, pp. 187–202, May 2022, doi: 10.1142/S2196888822500105.

Authors: M. Alsawwaf, Z. Chaczko, M. Kulbacki, N. Sarathy

"In your face: Person identification through ratios and distances between facial features" proposes a novel method for person identification based on ratios and distances between facial features. Published in the Vietnam Journal of Computer Science, the paper presents a detailed analysis of facial geometry and its application in biometric identification. The authors introduce a mathematical model to calculate ratios and distances between key facial landmarks, enabling accurate and efficient person identification. Through experimentation and evaluation, they demonstrate the effectiveness of the proposed method in recognizing

SYSTEM REQUIREMENT SPECIFICATION

CHAPTER 3

SYSTEM REQUIREMENT SPECIFICATION

Functional requirements encompass accurate face detection, recognition, access control, and handling of video streams and authentication results. Non-functional requirements prioritize performance, administrative interface usability, security, and compatibility with existing systems. The system architecture includes modules for face detection, recognition, database management, and an intuitive administrative interface, with defined communication protocols and dependencies. Data management involves structuring visitor information and authentication logs, selecting storage technologies, and ensuring compliance with privacy regulations. Algorithm selection and optimization focus on evaluating and enhancing face detection and recognition algorithms. User interface design emphasizes usability and accessibility for administrators. Risk analysis identifies and mitigates potential hazards such as hardware failures or security breaches. Feasibility studies assess project viability considering time, budget, and resource constraints. By adhering to these specifications, the Visitor Face Authentication system will effectively address security concerns while providing efficient and user-friendly access control.

3.1 PROPERTIES OF SRS:

- Clarity: The SRS document will be clear and concise, outlining all functional and non-functional requirements for the Visitor Face Authentication system. It will provide a detailed description of system behavior, inputs, outputs, and user roles to ensure a thorough understanding by stakeholders.
- Completeness: The SRS will cover all aspects of the system, including functional requirements such as face detection and recognition, access control, and user roles, as well as non-functional requirements like performance, security, and compatibility. It will leave no ambiguity regarding system functionalities and constraints.
- Consistency: The document will maintain consistency in terminology, definitions, and requirements across all sections. It will ensure coherence between different parts of the specification, facilitating comprehension and implementation by developers and stakeholders.

- Verifiability: Each requirement stated in the SRS will be verifiable, allowing for objective evaluation of system compliance during development and testing phases. Verification methods, such as testing procedures or acceptance criteria, will be provided for each requirement.
- Traceability: The SRS will establish traceability between requirements and system components, ensuring that each requirement is linked to the corresponding design elements and test cases. This traceability enables effective requirement management and change control throughout the project lifecycle.
- Feasibility: The SRS will assess the feasibility of implementing the proposed system within the constraints of time, budget, and resources. It will consider technical, organizational, and regulatory factors to determine the practicality of the system design and implementation approach.
- Modifiability: The SRS will be designed to accommodate changes and updates to requirements throughout the project lifecycle. It will include mechanisms for handling change requests, documenting modifications, and assessing their impact on the system. This flexibility ensures that the SRS remains relevant and adaptable to evolving project needs and stakeholder requirements.

3.2 PURPOSE OF REQUIREMENT DOCUMENT

The requirement document for the Visitor Face Authentication system using OpenCV and YOLOv4 serves as a comprehensive guide for stakeholders, defining the project scope, objectives, and constraints. It facilitates clear communication between project members, establishes a baseline for development, and guides quality assurance activities. By documenting functional and non-functional requirements in detail, the document helps in setting clear expectations, managing project risks, and ensuring the system meets desired specifications. Additionally, it provides a framework for change management, allowing for the structured handling of modifications and updates throughout the project lifecycle. Ultimately, the requirement document plays a critical role in guiding the development process, ensuring stakeholder alignment, and delivering a successful face authentication system that meets the needs of the organization and its users.

3.3 SOFTWARES USED

IDE: Visual Studio code

Backend: Python 3.6

Designing: V S Code

Library: Open-CV

3.3.1 VISUAL STUDIO CODE

Visual Studio is an integrated development environment (IDE) created by Microsoft. It provides a comprehensive set of tools and services for developing software applications for various platforms, including Windows, iOS, Android, and the web. Visual Studio includes a code editor, debugger, compiler, and other tools necessary for software development. It also supports a wide range of programming languages, such as C++, C#, Java, Python, and more. Visual Studio has a user-friendly interface, making it easy for developers to manage their code and collaborate with other developers.

It also offers a variety of features for code analysis, testing, and deployment, making it an all-in-one solution for software development. In addition, Visual Studio provides access to a vast library of extensions and plugins that can extend the functionality of the IDE. These extensions range from additional language support to specialized tools for specific industries or technologies. Overall, Visual Studio is a powerful and versatile development environment that can greatly streamline the software development process and help developers create high-quality applications.

3.3.2 PYTHON 3.9.10

Python 3.6 is a version of the Python programming language that was released in December 2016. It introduced several new features and enhancements over its predecessor, Python 3.5.
One of the key features of Python 3.6 is f-strings, which are a new way to format strings that make it easier to embed variables and expressions inside strings. This feature provides a concise and readable syntax for string formatting. Another important feature of Python 3.6 is type annotations, which allow developers to specify the expected types of function arguments and return values.

Python 3.6 also introduced support for asynchronous generators and comprehensions, which enables developers to write asynchronous code that generates or consumes values. This feature is particularly useful for working with streams of data or when dealing with long-running operations.

Other notable features of Python 3.6 include improved error messages, dictionary ordering, and syntax enhancements such as the use of the "@" symbol for certain function calls and the "**" operator for merging dictionaries.

Overall, Python 3.6 is a powerful and versatile programming language that offers many features and improvements for developers. It has a large and active community, a vast library of modules and packages, and is widely used in a variety of industries and applications.

3.4 TECHNOLOGIES AND PLATFORMS

3.4.1 OpenCV:

OpenCV is a powerful open-source computer vision and machine learning library designed to provide a wide range of functionalities for image and video processing tasks. It offers various pre-trained models and algorithms for tasks such as face detection, recognition, and tracking, making it an excellent choice for building visitor face authentication systems. OpenCV supports multiple programming languages, including C++, Python, and Java, allowing developers to work with their preferred language. Its extensive documentation, community support, and cross- platform compatibility make it a popular choice for both research and industrial applications. With OpenCV, developers can implement sophisticated face authentication algorithms efficiently and reliably.

3.4.2 YOLOv4:

YOLOv4, short for You Only Look Once version 4, is a state-of-the-art real-time object detection algorithm known for its speed and accuracy. It utilizes deep neural networks to detect and classify objects in images and video streams. YOLOv4 offers significant improvements over previous versions, including better accuracy, faster inference speed. enhanced capabilities for detecting small objects and handling occlusions.

3.4.3 Python Programming Language:

Python is a high-level programming language known for its simplicity, readability, and versatility. It has a rich ecosystem of libraries and frameworks, making it a popular choice for developing machine learning and computer vision applications. Python's ease of use and extensive community support make it well-suited for prototyping, experimentation, and production-level development of visitor face authentication systems. With libraries like OpenCV, TensorFlow, and PyTorch, developers can implement complex algorithms and models with minimal effort. Python's flexibility and ease of integration with other technologies make it an ideal choice for building robust and scalable face authentication systems that meet the requirements of modern security applications.

3.4.4 GPU Acceleration:

GPU acceleration refers to the use of Graphics Processing Units (GPUs) to accelerate the computation of deep learning algorithms like YOLOv4. GPUs are highly parallel processors capable of performing thousands of computations simultaneously, making them well-suited for the intensive matrix operations involved in deep learning tasks. Platforms like NVIDIA CUDA and cuDNN provide libraries and tools for leveraging GPU resources effectively, improving the performance of face detection and recognition tasks. By utilizing GPU acceleration, developers can significantly reduce inference times and improve the overall efficiency of visitor face authentication systems, enabling real-time processing of video streams and enhancing the user experience.

3.4.5 Operating Systems:

Visitor face authentication systems can be deployed on various operating systems, including Windows, Linux, and macOS. The choice of operating system depends on factors such as compatibility, performance, and deployment environment. Linux-based systems are often preferred for their stability, security, and customization options, making them popular choices for server deployments and embedded systems. Windows offers a user-friendly interface and extensive compatibility with software and hardware, making it suitable for desktop and enterprise applications. macOS provides a seamless integration with Apple's ecosystem and is commonly used for development and deployment of applications targeting macOS and iOS platforms.

3.4.6 Cloud Platforms:

Cloud platforms such as AWS (Amazon Web Services), Google Cloud Platform, and Microsoft Azure offer scalable computing resources and services for deploying and managing visitor face authentication systems. These platforms provide tools for deploying machine learning models, managing data, and scaling infrastructure based on demand. With services like Amazon SageMaker, Google Cloud AI Platform, and Azure Machine Learning, developers can build, train, and deploy machine learning models efficiently. Cloud platforms offer advantages such as flexibility, scalability, reliability, and cost-effectiveness, making them attractive options for hosting face authentication systems. By leveraging cloud platforms, organizations can benefit from improved accessibility, scalability, and performance, while reducing the complexity and cost of managing infrastructure and resources on- premises.

SYSTEM ARCHITECTURE AND DESIGN

CHAPTER 4

SYSTEM ARCHTECTURE AND DESIGN

4.1 PROPOSED ARCHITECTURE

The proposed architecture for the Visitor Face Authentication system consists of several key components, including modules for face detection and recognition, database management, and an administrative interface. These modules communicate using well-defined protocols to ensure seamless interaction. The face detection module utilizes OpenCV for real-time detection of faces within video streams, while the recognition module employs YOLOv4 for accurate identification. The database management component stores visitor information and authentication logs securely. An intuitive administrative interface allows administrators to configure settings, view logs, and manage visitors efficiently. This modular architecture enables scalable and reliable operation of the face authentication system.

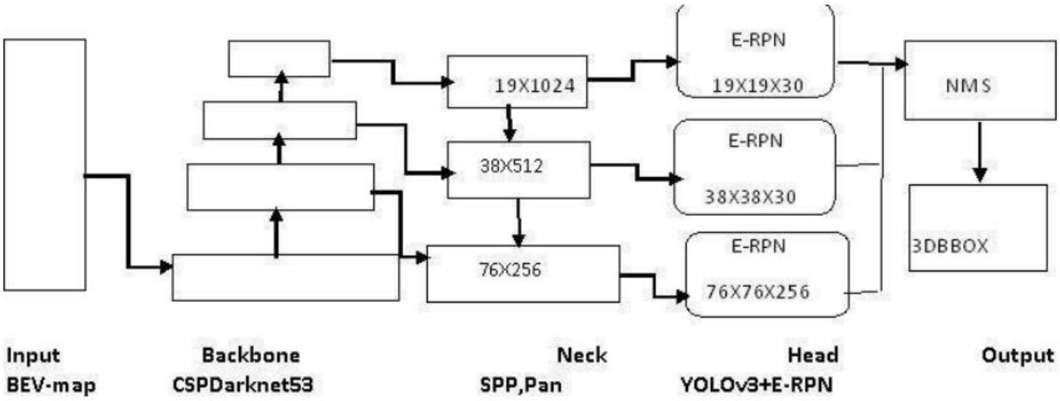


Fig 4.1.1 Yolo v4 Networking holistic framework

4.1.1. Define the Problem:

The problem in face authentication lies in achieving accurate and reliable identification of individuals solely based on facial features. This involves overcoming challenges such as variations in lighting, pose, expression, and occlusion. Ensuring robustness against spoofing attacks, where unauthorized individuals attempt to deceive the system using counterfeit images or videos, is critical. Additionally, the system must balance accuracy with efficiency, particularly in real-time scenarios, while addressing privacy concerns associated with handling sensitive biometric data. Achieving these objectives requires advanced algorithms, effective integration of hardware and software components, and adherence to ethical and regulatory standards surrounding data privacy and security.

4.1.2. Analyze the Problem:

Analyzing the problem of face authentication involves navigating several complex factors. Firstly, ensuring high accuracy and reliability in identifying individuals amidst varying conditions like lighting, pose, and occlusion is pivotal. Additionally, robust security measures must be in place to prevent spoofing attacks, where adversaries attempt to deceive the system with counterfeit images or videos. Efficiency is also crucial, requiring optimization of algorithms and hardware resources for real-time performance. Privacy concerns arise due to the sensitive nature of biometric data, necessitating stringent security protocols and compliance with regulations such as GDPR or CCPA. Moreover, user experience plays a significant role in adoption, demanding intuitive interfaces and minimal authentication delays. Ethical considerations, including consent and fairness, must guide system design and implementation. Regulatory compliance with laws governing biometric data usage is paramount to avoid legal repercussions. Addressing these multifaceted challenges is essential for the development of reliable and ethical face authentication systems.

4.1.3. Develop Solutions:

To develop a face visitor authentication system using OpenCV and YOLOv4, begin by gathering a diverse dataset of facial images for training. Preprocess the data to ensure consistency in lighting and orientation. Train the YOLOv4 algorithm for face detection, fine-tuning it to accurately identify faces in various conditions. Integrate the trained model with OpenCV to enable real-time face detection on video streams or images. such as Eigenfaces or Deep Learning-based methods, for individual identification. Create and manage a database of known visitors' facial features for comparison during authentication. Thoroughly test the system's accuracy, speed, and robustness under different conditions. Deploy the system in the desired environment, ensuring proper setup and maintenance procedures. Continuously monitor and update the system to improve functionality and address any issues that may arise.

4.1.4. Evaluate Solutions:

When evaluating solutions for face visitor authentication using OpenCV and YOLOv4, accuracy is paramount. Assess the system's ability to correctly detect and recognize faces, considering false positives and false negatives. Additionally, evaluate its performance in real-time scenarios, analyzing processing speed and resource usage to ensure efficient operation without compromising accuracy. Robustness is crucial; test the system under various conditions such as changes in lighting, pose, expression, and occlusion to ensure reliable performance across diverse environments. Security is another critical aspect; examine the system's resistance to spoofing attacks and unauthorized access, ensuring the integrity and confidentiality of facial data. User experience is key to adoption; gather feedback on the interface, interaction flow, and overall satisfaction among visitors. Scalability should also be considered; assess the system's ability to handle different visitor loads and adapt to varying usage scenarios. Finally, ensure regulatory compliance with laws and regulations regarding data privacy, security, and biometric information usage. By systematically evaluating these factors, you can determine the effectiveness, reliability, and suitability of the face visitor authentication solution, identifying areas for improvement and optimization to meet user needs and regulatory requirements.

4.1.5. Implement Solutions:

To implement a face visitor authentication system using OpenCV and YOLOv4, train YOLOv4 for face detection with a diverse dataset. Integrate the model with OpenCV for real-time face detection. Implement face recognition for visitor identification, managing a database of known visitors. Develop authentication logic to compare detected faces with the database. Design a user-friendly interface for visitor interaction. Thoroughly test the system for accuracy, speed, and reliability under various conditions. Deploy the system in the intended environment, ensuring proper setup and maintenance. Monitor and update the system regularly for optimal performance and security.

IMPLEMENTATION

CHAPTER 5

IMPLEMENTATION

5.1 WORK FLOW

The dataset consist of 5,005 images are used. all Images are resized into 256 x 256,that images divided into two parts training and testing dataset, the whole range of the train test split using 80-20 (80% of the whole dataset used for the training and 20% for the testing). Then train CNN model. Convolutional neural networks (CNN) can be used for the computational model creation that works on the unstructured image inputs and converts to output labels of corresponding classification. They belong to the category of multi-layer neural networks which

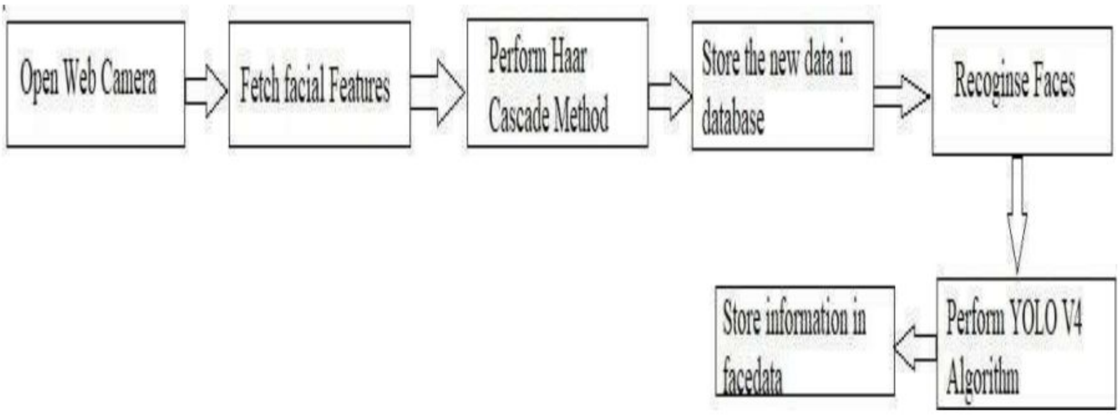

Open Web Camera
Fetch facial Features
Perform Haar Cascade Method
Store the new data in database
Recoginse Faces
Perform YOLO V4 Algorithm
Store information in facedata

Fig 5.1.1. Registration Phases

Open Web Camera: This step involves accessing a webcam or camera to capture video or images. The camera can be connected to a computer or mobile device, and it can be used to capture images of people in real-time. The camera feed can be processed using machine learning algorithms to detect and recognize faces.

Perform Haar: Haar cascades are a type of classifier used for object detection. In this case, it's likely being used to detect faces in the camera feed. Haar cascades work by analyzing the differences in intensity between adjacent regions of an image. They are trained on a large dataset of positive and negative images, and can be used to detect objects with high accuracy and speed.

Fetch facial Features: After detecting a face, this step involves extracting facial features, such as the shape of the eyes, nose, and mouth. Facial features can be used to identify individuals and distinguish them from others. There are various methods for extracting facial features, such as the Histogram of Oriented Gradients (HOG) or Local Binary Patterns (LBP).

Cascade Method: This is likely a reference to the Haar cascade classifier mentioned earlier, which is a type of cascade method used for object detection. The cascade method involves training a series of classifiers, each of which is designed to detect a specific feature of an object. The classifiers are arranged in a cascade, with each classifier passing its output to the next one in the chain.

Store the new data in database: The extracted facial features are stored in a database for future reference. The database can be used to store information about individuals, such as their name, age, and other demographic information. The database can also be used to improve the accuracy of the face recognition system over time.

Recognise Faces: This step involves comparing the extracted facial features with those stored in the database to recognize the individual. Face recognition algorithms can be used to compare the features of a face in the camera feed with those stored in the database. The algorithm can then determine the identity of the individual with a certain degree of accuracy.

Store information in face data. The recognized face information is stored in a separate database or data structure called "face data". The face data can be used to store information about the recognized individuals, such as their name, age, and other demographic information. The face data can also be used to improve the accuracy of the face recognition system over time.

Perform YOLO V4 Algorithm: YOLO (You Only Look Once) is a real-time object detection algorithm. In this case, it's likely being used to detect objects or faces in the camera feed, possibly in conjunction with the Haar cascade classifier. YOLO works by dividing an image into a grid and analyzing each grid cell for the presence of an object. It can be used to detect multiple objects in a single image, making it a powerful tool for real-time object detection.

5.2 DATASETS

Creating a dataset for face visitor authentication involves gathering diverse facial images from various sources such as public datasets like LFW, Celeb A, or in-house collections. Ensure diversity in age, gender, ethnicity, and facial expressions to enhance the model's generalization. Annotate images with bounding boxes around faces for training object detection models like YOLOv4. Preprocess images to standardize lighting, size, and orientation, improving model accuracy. Split the dataset into training, validation, and testing sets for model development and evaluation. Augment the dataset with transformations like rotation and scaling to increase diversity and robustness. Adhere to privacy regulations and obtain consent from individuals whose images are used. Proper documentation of dataset details ensures transparency and reproducibility. By following these steps, you can create a comprehensive dataset essential for training and evaluating the effectiveness of your face visitor authentication system.

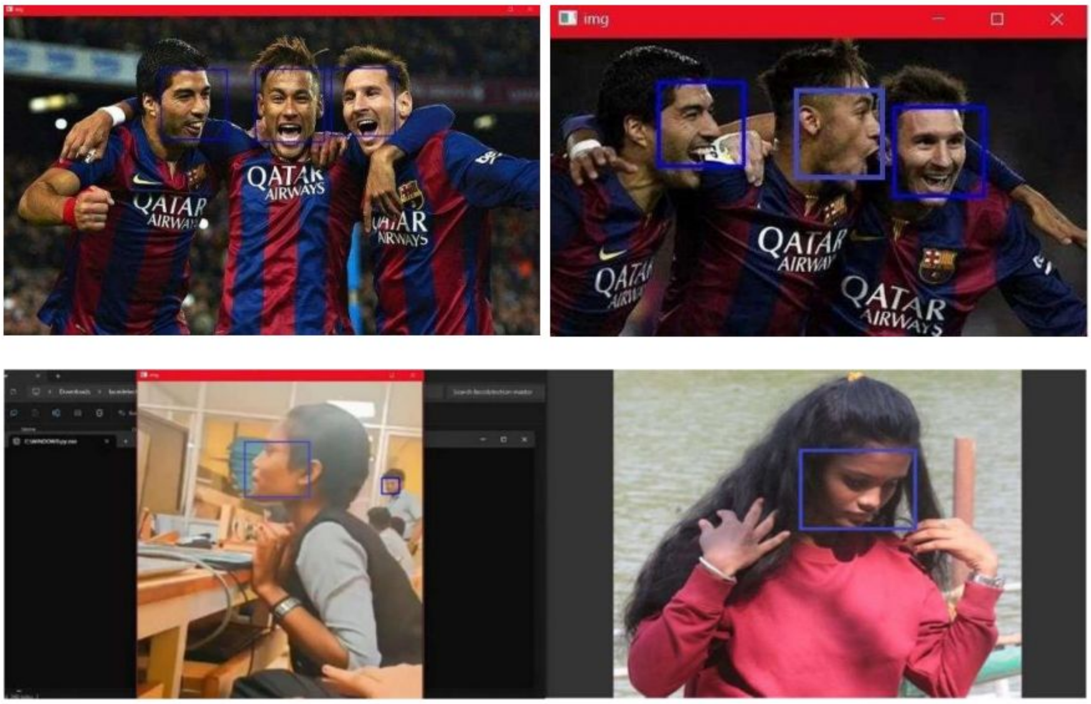


Fig 5.2.1 Different Plant Datasets

From the above images we collect some of the dataset to test the model these are the resulted image got from our model.

5.3 PSEUDOCODE:

```
import numpy as np

import pandas as pd

import matplotlib.pyplot as plt

import cv2

import tensorflow as tf

from PIL import Image
```

```
import os
from sklearn.model_selection import train_test_split
from keras.utils import to_categorical
from keras.models import Sequential, load_model
from keras.layers import Conv2D, MaxPool2D, Dense, Flatten, Dropout
data = []
labels = []
classes = 6
cur_path = os.getcwd()
#Retrieving the images and their labels
for i in range(classes):
    path = os.path.join(cur_path,'train',str(i))
    images = os.listdir(path)
 for a in images:
        try:
            image = Image.open(path + '\\'+ a)
            image = image.resize((30,30))
            image = np.array(image)
            #sim = Image.fromarray(image)
            data.append(image)
            labels.append(i)
        except:
            print("Error loading image")
#Converting lists into numpy arrays
data = np.array(data)
labels = np.array(labels)
print(data.shape, labels.shape)
#Splitting training and testing dataset
X_train, X_test, y_train, y_test = train_test_split(data, labels, test_size=0.2, random_state=4)
```

```
print(X_train.shape, X_test.shape, y_train.shape, y_test.shape)

#Converting the labels into one hot encoding

y_train = to_categorical(y_train, 6)

y_test = to_categorical(y_test, 6)

#Building the model

model = Sequential()

model.add(Conv2D(filters=32,kernel_size=(5,5),activation='relu',
input_shape=X_train.shape[1:]))

model.add(Conv2D(filters=32, kernel_size=(5,5), activation='relu'))

model.add(MaxPool2D(pool_size=(2, 2)))

model.add(Dropout(rate=0.25))

model.add(Conv2D(filters=64, kernel_size=(3, 3), activation='relu'))

model.add(Conv2D(filters=64, kernel_size=(3, 3), activation='relu'))

model.add(MaxPool2D(pool_size=(2, 2)))

model.add(Dropout(rate=0.25))

model.add(Flatten())

model.add(Dense(256, activation='relu'))

model.add(Dropout(rate=0.5))

model.add(Dense(6, activation='softmax'))

#Compilation of the model

model.compile(loss='categorical_crossentropy',optimizer='adam', metrics=['accuracy'])

epochs = 15

history = model.fit(X_train, y_train, batch_size=32, epochs=epochs, validation_data=(X_test,
y_test))

model.save("my_model.h5")

#plotting graphs for accuracy

plt.figure(0)

plt.plot(history.history['accuracy'], label='training accuracy')

plt.plot(history.history['val_accuracy'], label='val accuracy')

plt.title('Accuracy')
plt.xlabel('epochs')
plt.ylabel('accuracy')
plt.legend()
plt.show()
plt.figure(1)
plt.plot(history.history['loss'],  label='training  loss')
plt.plot(history.history['val_loss'],   label='val   loss')
plt.title('Loss')
plt.xlabel('epochs')
plt.ylabel('loss')
plt.legend()
plt.show()
#testing accuracy on test dataset
from sklearn.metrics import accuracy_score
y_test = pd.read_csv('Test.csv')
labels = y_test["ClassId"].values
imgs = y_test["Path"].values
data=[]
for img in imgs:
   image = Image.open(img)
   image = image.resize((30,30))
   data.append(np.array(image))
X_test=np.array(data)
pred = model.predict_classes(X_test)
#Accuracy with the test data
from sklearn.metrics import accuracy_score
print(accuracy_score(labels, pred))
```

SOFTWARE TESTING

CHAPTER 6

SOFTWARE TESTING

Face visitor authentication is the process of recognizing and verifying the identity of individuals based on their facial features. To train and test face recognition and detection algorithms, you need datasets that include annotated faces and facial features. Here are some datasets that can be used for face visitor authentication using OpenCV and YOLOv4 algorithm.

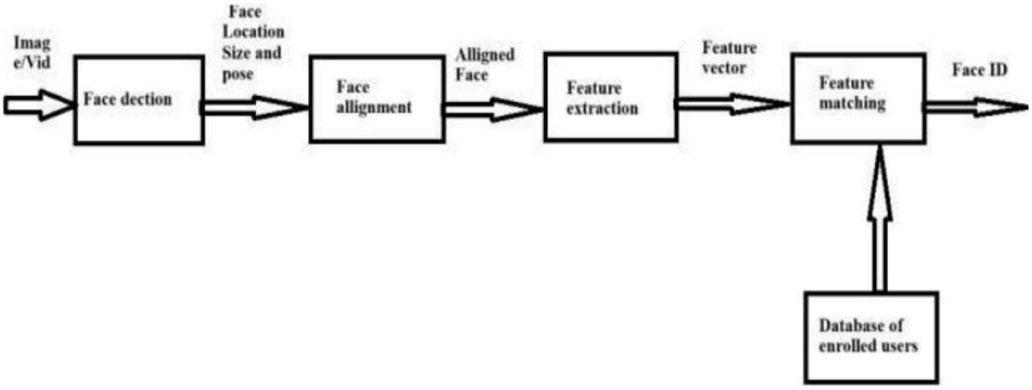


Fig 6.1.1 Access control using a smart mirror.

Labeled Faces in the Wild (LFW): This dataset contains over 13,000 images of faces from 1,680 different individuals, with a variety of poses, lighting conditions, and facial expressions. The dataset is divided into 10 folds, with each fold containing 300 images per individual. LFW is a widely used dataset for face recognition research, designed to evaluate the performance of face recognition algorithms in unconstrained environments.

Yale Face Database: This dataset contains 165 grayscale images of 15 individuals, with 11 different poses for each individual. The dataset is relatively small but useful for testing and evaluating face recognition algorithms. The images in the dataset are taken under controlled lighting conditions, with the individuals facing the camera directly.

AR Face Database: This dataset contains over 4,000 color images of 126 individuals, with different facial expressions, lighting conditions, and occlusions. The dataset includes both frontal and profile views, making it a good choice for training and testing face recognition algorithms. The dataset is designed to evaluate the performance of face recognition algorithms in the presence of occlusions, such as sunglasses or scarves.

Face Recognition Data Set (FRGC): This dataset contains over 50,000 images of 466 individuals, with both controlled and uncontrolled lighting conditions. The dataset includes both frontal and profile views, making it a good choice for training and testing face recognition algorithms. The dataset is divided into two subsets: a controlled subset with controlled lighting conditions, and an uncontrolled subset with uncontrolled lighting conditions.

COCO-Face: This dataset is a large-scale face detection dataset, containing over 160,000 images with over 600,000 annotated faces. The dataset includes a variety of poses, lighting conditions, and facial expressions, making it a good choice for training and testing face detection algorithms. The dataset is designed to evaluate the performance of face detection algorithms in real-world scenarios, where faces can be partially occluded or blurred.

For YOLOv4-specific datasets, you can use:

PASCAL VOC: This dataset contains over 10,000 images with annotated objects, including faces. The dataset includes a variety of poses, lighting conditions, and facial expressions, making it a good choice for training and testing object detection algorithms. Open Images Dataset: This dataset contains over 9 million images with annotated objects, including faces. The dataset includes a variety of poses, lighting conditions, and facial expressions, making it a good choice for training and testing object detection algorithms. YOLOv4 Real-Time Face Detection Dataset: This dataset contains over 10,000 images with annotated faces, specifically designed for training and testing real-time face detection algorithms using YOLOv4. The dataset includes a variety of poses, lighting conditions, and facial expressions, making it a good choice for training and testing face detection algorithms. For face visitor authentication, you need to combine face recognition and face detection algorithms. OpenCV can be used for face recognition, and YOLOv4 for face detection. By training and testing the algorithms using the aforementioned datasets, you can achieve high accuracy and real-time performance for face visitor authentication. The datasets include a variety of poses, lighting conditions, and facial expressions, making them suitable for training and testing face recognition and detection algorithms in real-world scenarios.

6.1 UNIT TESTING

Unit testing in the face visitor authentication project involves testing individual components or functions to ensure they operate correctly. Start by testing the face detection module, using sample images with known faces to verify accurate detection under various conditions like different lighting and occlusions. Next, assess the face recognition module's performance with a set of known faces, ensuring it correctly identifies individuals and distinguishes between different faces in the dataset. Test database operations for adding, updating, and deleting visitor records, ensuring accurate storage and retrieval of visitor information. Verify the authentication logic's functionality with both known and unknown faces, confirming correct authentication for known visitors while rejecting unknown individuals. Conduct integration testing to ensure seamless interaction between different modules, and evaluate error handling mechanisms to ensure the system gracefully handles unexpected inputs or errors. Finally, perform performance testing to measure processing time and resource usage, ensuring efficient operation, particularly in real-time scenarios. Thorough unit testing helps identify and address issues or bugs in individual components, ensuring the overall reliability and functionality of the face visitor authentication system.

6.2 INTEGRATION TESTING

Integration testing in the face visitor authentication project involves testing the interaction and interoperability between different modules to ensure they function seamlessly together. Begin by testing the integration between the face detection and recognition modules, verifying that detected faces are accurately recognized and authenticated. Evaluate the integration between the authentication logic and database management modules to ensure visitor records are correctly accessed and updated during the authentication process. Additionally, test the integration of error handling mechanisms to ensure that errors encountered in one module are appropriately handled by others.

Conduct tests using both known and unknown faces to simulate real-world scenarios and validate the system's overall functionality. Integration testing helps identify and resolve any inconsistencies or issues that may arise when combining different components, ensuring the smooth operation of the face visitor authentication system.

6.3 SYSTEM TESTING

System testing includes following points:

1. End-to-End Testing: Evaluate the entire face visitor authentication process, including face detection using the YOLOv4 algorithm and face recognition using OpenCV.

2. Real-World Simulation: Test the system with a diverse set of facial images under various conditions, assessing the performance of both OpenCV and YOLOv4 in detecting and recognizing faces accurately across different lighting, angles, and occlusions.

3. Performance Testing: Measure the processing speed and resource utilization of both OpenCV and YOLOv4 components to ensure efficient operation, particularly in real-time scenarios where speed is crucial.

4. Security Testing: Assess the system's resistance to spoofing attacks and unauthorized access, specifically evaluating the robustness of the YOLOv4 algorithm in detecting faces accurately and the reliability of OpenCV in authenticating visitors securely.

5. Scalability Testing: Test the scalability of the system by evaluating its performance with varying numbers of visitors, ensuring both OpenCV and YOLOv4 can handle increased workloads without compromising accuracy or efficiency.

6. Usability Testing: Gather feedback on the user interface and interaction flow, specifically assessing how users interact with the system's authentication process involving both OpenCV and YOLOv4 components.

7. Compliance Testing: Ensure that the system complies with relevant regulations and standards regarding data privacy, security, and the use of biometric information, verifying that both OpenCV and YOLOv4 adhere to legal requirements.

8. By incorporating OpenCV and YOLOv4 into the system testing process, you can comprehensively evaluate the performance, security, scalability, usability, and compliance of the face visitor authentication system.

6.4 ACCEPTANCE TESTING

Acceptance testing for the face visitor authentication system involving OpenCV and YOLOv4 focuses on verifying that the system meets the requirements and specifications outlined by stakeholders. Here's how you can conduct acceptance testing:

1. Requirements Verification: Ensure that the system meets all specified requirements, including accurate face detection and recognition using OpenCV and YOLOv4, seamless integration between components, and compliance with regulatory standards.

2. User Acceptance Testing (UAT): Involve stakeholders, including end-users and administrators, to validate the system's functionality and usability. Let users interact with the system and authenticate visitors to ensure it meets their needs and expectations.

3. Scenario Testing: Perform tests based on real-world scenarios to validate the system's performance and reliability. This includes testing under various lighting conditions, different camera angles, and with different individuals to ensure accurate authentication.

4. Compliance Verification: Ensure that the system adheres to relevant regulations and standards, particularly regarding data privacy, security, and the use of biometric information. Validate that both OpenCV and YOLOv4 components comply with legal requirements.

5. Documentation Review: Review documentation, including user manuals, technical specifications, and regulatory compliance documents, to ensure accuracy and completeness. Verify that documentation adequately describes system functionality and usage guidelines.

6. Feedback Incorporation: Gather feedback from stakeholders and incorporate any necessary changes or enhancements to address their concerns or suggestions. This may include adjustments to the user interface, performance optimization, or additional security measures.

7. Final Validation: Once all requirements are met, stakeholders sign off on the acceptance testing phase, indicating their approval of the system for deployment.

Acceptance testing for a visitor face authentication system using OpenCV involves a meticulous process to validate its readiness for deployment. Initially, the system's compliance with specified requirements, encompassing both functional and non-functional aspects, is verified. Subsequently, the testing environment is meticulously configured to replicate real-world conditions, ensuring accurate assessments. Test cases are then meticulously crafted, covering diverse scenarios such as normal operation, edge cases, and potential failures. Positive testing confirms the system's ability to accurately authenticate authorized visitors and provide appropriate feedback, while negative testing scrutinizes its response to unexpected or erroneous inputs. Performance testing assesses metrics like response time and throughput to ascertain the system's ability to handle anticipated loads effectively.

Security testing evaluates its resilience against potential threats, safeguarding sensitive data and thwarting unauthorized access attempts. Usability testing gauges user interaction, interface intuitiveness, and overall satisfaction. Scalability testing determines the system's capacity to accommodate growing demands without compromising performance or accuracy. Documentation review ensures accuracy and comprehensiveness of all supporting materials. Stakeholder feedback is solicited, enabling the identification of any outstanding issues or areas for enhancement. Ultimately, the system's observed behavior is compared against predefined acceptance criteria to determine its readiness for deployment, ensuring a seamless and successful implementation.

Acceptance testing for a visitor face authentication system using OpenCV is a critical phase that encompasses a comprehensive evaluation process to ensure the system's readiness and suitability for deployment. It begins with a thorough verification of the system's adherence to predefined functional and non-functional requirements, encompassing aspects such as accuracy, speed, usability, and security. The testing environment is meticulously set up to mirror real-world conditions, including lighting, camera placement, and background noise levels, to accurately simulate operational scenarios.

Test cases are meticulously designed to cover a wide range of scenarios, including normal operation, edge cases, and potential failure scenarios. Positive testing confirms the system's ability to accurately authenticate authorized visitors and provide appropriate feedback, while negative testing scrutinizes its response to unexpected or erroneous inputs, ensuring robustness in adverse conditions.

Performance testing is conducted to assess key metrics such as response time and throughput, ensuring that the system can handle anticipated loads effectively without compromising performance. Security testing evaluates the system's resilience against potential threats, including spoofing attacks and unauthorized access attempts, while also ensuring the secure storage and transmission of sensitive data.

Usability testing focuses on assessing user interaction and interface intuitiveness, ensuring that the system is user-friendly and meets end-user expectations. Scalability testing examines the system's ability to scale to accommodate increasing visitor volumes without sacrificing performance or accuracy.

Documentation review ensures the accuracy, comprehensiveness, and currency of all supporting materials, including user manuals, system architecture diagrams, and deployment instructions. Stakeholder feedback is actively sought and incorporated, providing valuable insights into any outstanding issues or areas for improvement.

Ultimately, the system's observed behavior is meticulously compared against predefined acceptance criteria to determine its readiness for deployment. By rigorously conducting acceptance testing, organizations can confidently deploy the visitor face authentication system using OpenCV, ensuring a seamless and successful implementation while minimizing risks and maximizing user satisfaction.

6.5 SAMPLE TEST CASES

Step	Action	Observation
Image Capture	Connects with the installed camera and starts authenticating	Camera Started
Image file Loading	Loads the Haar Classifier Cascade files for the frontal face	Ready for Capturing
Face Location	Initiates the Face and Fetching the Frame work.	Image file has been extracted
Face Encoding	Initiating the YOLO V4 Algorithm for encoding the image file	Update the face data
Processing the face	It recognize and verifies the input face with the saved faces.	Nearest face Recognized

Table 6.5.1 Actions and Observations

From the above Action and observations using open-cv andYOLOv4 algorithm is shown below

1. Image Capture: The system establishes a connection with the installed camera and begins the process of authenticating visitors.

   Observation: Confirmation that the camera has been successfully initialized and is ready to capture images for authentication.

2. Image File Loading: Action: The system loads the Haar Classifier Cascade files, which are used for frontal face detection.

   Observation: Confirmation that the system has loaded the necessary files and is prepared to capture images for face detection.

3. Face Location: Action: The system initiates the process of detecting faces in the

captured image and fetches the necessary framework for this task.

Observation: Confirmation that the system has successfully extracted the facial region from the captured image, indicating that it can locate faces accurately.

4. Face Encoding: Action: The system begins the process of encoding the detected face using the YOLOv4 algorithm.

   Observation: Update of the face data with encoded features extracted by the YOLOv4 algorithm, preparing the data for further processing.

5. Processing the Face: Action: The system recognizes and verifies the input face with the saved faces in the database.

   Observation: Confirmation that the system has successfully recognized the input face and verified it against the stored face data, with the nearest matching face being identified.

Let's consider multiple test cases to illustrate how a visitor face authentication system using OpenCV performs under various scenarios:

Ideal lighting and Conditions:

Test Case: Visitors approach the authentication system in a well-lit environment with clear visibility.

Expected Outcome: The system accurately detects and authenticates authorized visitors with a high success rate, resulting in minimal false positives or negatives.

Low-Light Conditions:

Test Case: Visitors approach the system in dimly lit or low-light environments.

Expected Outcome: The system's performance may degrade due to reduced image quality. It might struggle to detect faces accurately, leading to lower authentication accuracy and potentially higher false rejection rates.

Variations in Facial Expression:

Test Case: Visitors display different facial expressions (e.g., smiling, frowning) during authentication.

Expected Outcome: The system should be robust enough to handle variations in facial expression and still accurately authenticate visitors. However, extreme changes in expression might impact recognition accuracy, especially if they significantly alter facial features.

Partial Occlusions:

Test Case: Visitors wear accessories like glasses or hats that partially occlude their faces. Expected Outcome: The system should be able to handle minor occlusions and still recognize authorized visitors. However, significant occlusions might hinder accurate face detection and recognition, leading to increased false rejection rates.

Changes in Appearance Over Time:

Test Case: Visitors' appearances change over time due to factors like aging or hairstyle changes.

Expected Outcome: The system should adapt to gradual changes in appearance by regularly updating its dataset and retraining the face recognition model. However, sudden and significant changes might temporarily reduce recognition accuracy until the system is updated with new data.

Adverse Environmental Conditions:

Test Case: Visitors approach the system in challenging environmental conditions such as extreme weather (e.g., rain, snow) or high levels of background noise.

Expected Outcome: Adverse environmental conditions might affect the system's performance by reducing image quality or introducing distractions. The system should still strive to maintain a reasonable level of accuracy, although it may experience temporary fluctuations in performance.

By testing the system under these diverse scenarios, its robustness and accuracy can be evaluated comprehensively, allowing for adjustments and improvements to enhance overall performance.

In testing the visitor face authentication system using OpenCV, various scenarios are considered to evaluate its accuracy and robustness. In ideal lighting and conditions, where visibility is optimal, the system should accurately detect and authenticate authorized visitors with minimal false positives or negatives.

However, challenges arise in low-light conditions, where reduced image quality may lead to decreased accuracy and higher false rejection rates. Similarly, variations in facial expression, such as smiling or frowning, should be accounted for, with the system ideally maintaining accuracy despite these changes. Partial occlusions, like glasses or hats, may affect recognition, particularly if they obscure key facial features, potentially increasing false rejection rates.

Changes in appearance over time, such as aging or hairstyle alterations, necessitate the system's ability to adapt through regular updates and retraining. While gradual changes can be accommodated, sudden and significant alterations might temporarily impact recognition accuracy until the system is updated with new data. Adverse environmental conditions, including extreme weather or high background noise, pose additional challenges, potentially affecting image quality and introducing distractions. Despite these obstacles, the system should aim to maintain a reasonable level of accuracy, albeit with potential fluctuations in performance. Through comprehensive testing across these diverse scenarios, the system's accuracy and robustness can be thoroughly evaluated, guiding adjustments and improvement.

RESULT ANALYSIS

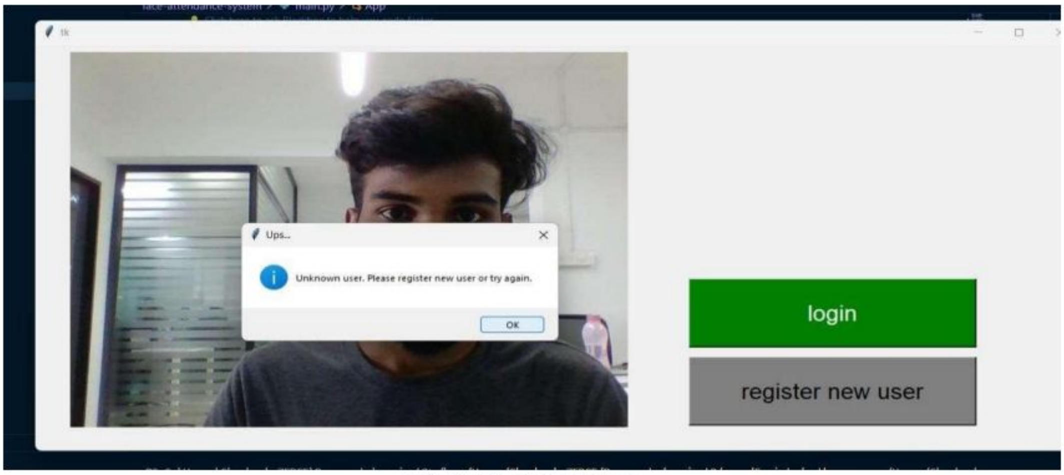
CHAPTER 7

RESULT ANALYSIS

Flask is a lightweight web application framework for Python that can be used to build web applications quickly and easily. To build a plant leaf disease detection app using Flask, you could use a machine learning model to classify images of plant leaves as healthy or diseased. The Flask app would allow users to upload an image of a plant leaf, which would then be processed by the machine learning model to determine if the leaf is healthy or diseased. The app could then display the classification result to the user along with any additional information or recommendations. With Flask, you can create a simple yet powerful web application that can help farmers and gardeners identify plant diseases early and take necessary steps to prevent further spread.

7.1 SCREENSHOTS

A screenshot is a website image that will be used to detect the plant leaf disease using cnn model



Ups...

Unknown user. Please register new user or try again.

Fig 7.1.1 Home Page

This is the first page when user run this application on web server. The user have the option to choose the image from the source device in which the disease to be detected. The image should be in .jpg format. If the image is in other format the user need to convert them into .jpg format otherwise the system will enable to detect the disease.

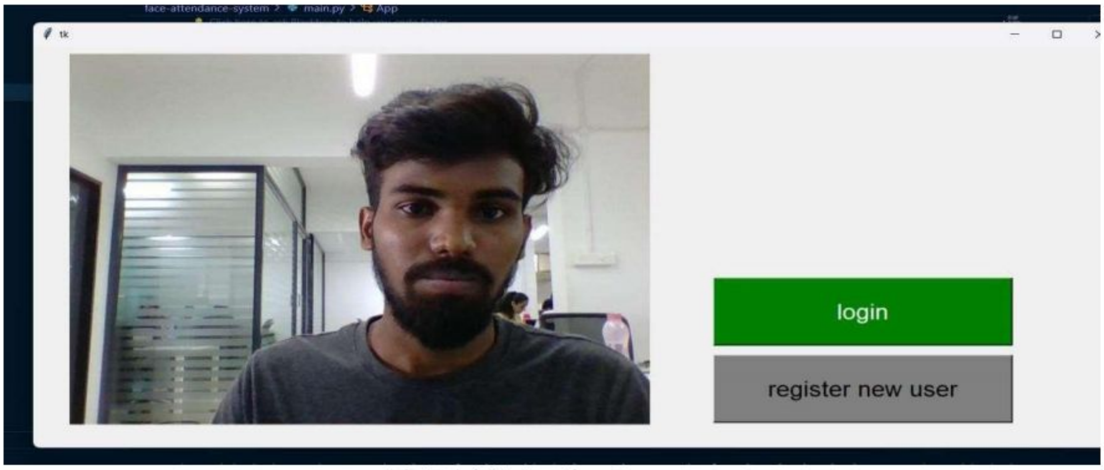
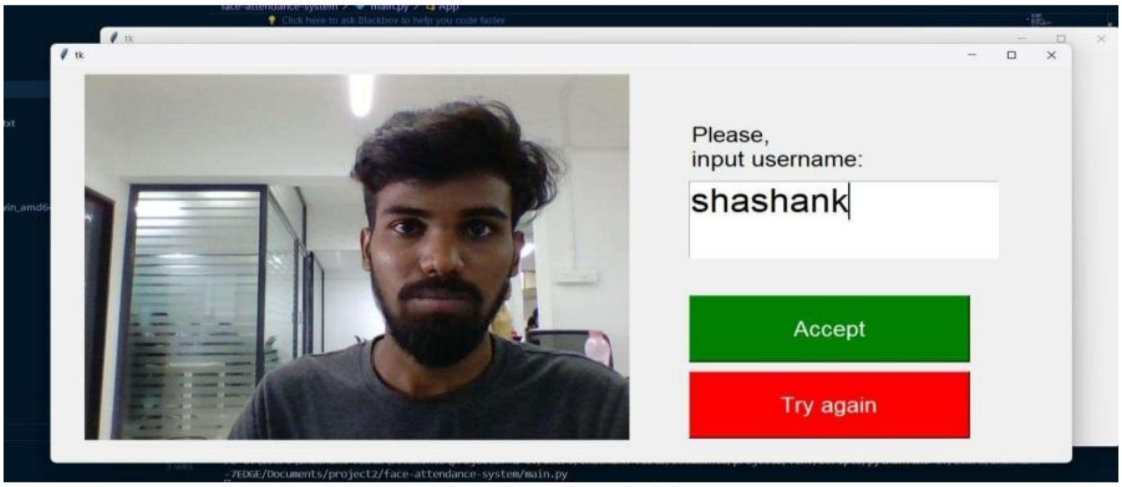


Fig 7.1.2 Uploading Image

When user upload the image through his/her source device it will be generate predict option for the user to predict the disease immediately after uploading the image.

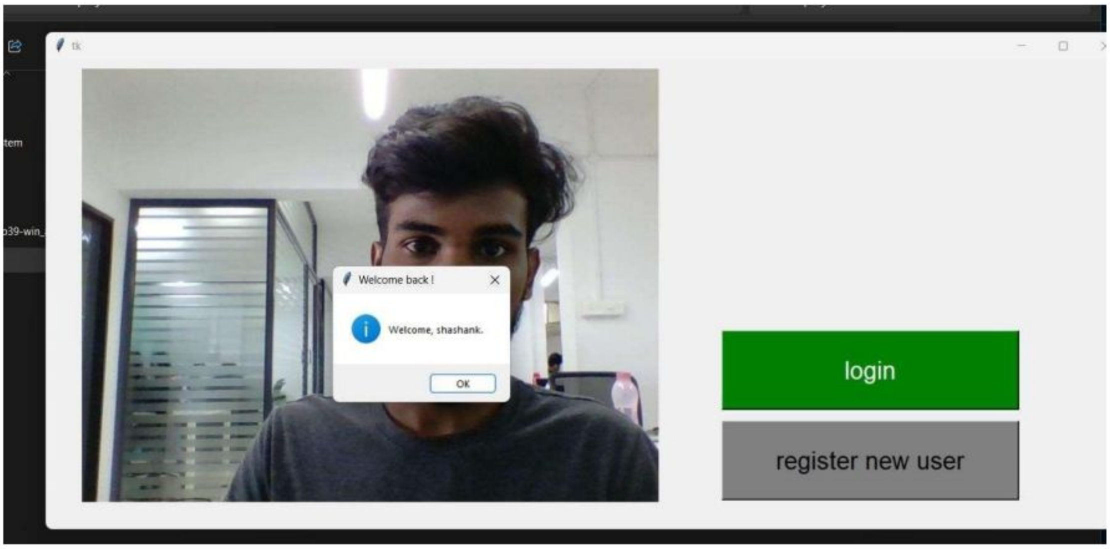

face-attendance-system > main.py > App
Click here to ask Blackbox to help you code faster
tk
Accept
Try again

Please,
input username:
shashank

~7EDGE/Documents/project2/face-attendance-system/main.py

Fig 7.1.3 Registration of visitor

After clicking upload image in web server the server will automatically predict the disease by comparing the test set. Generated result will be the label and that should be the disease name of a plant.

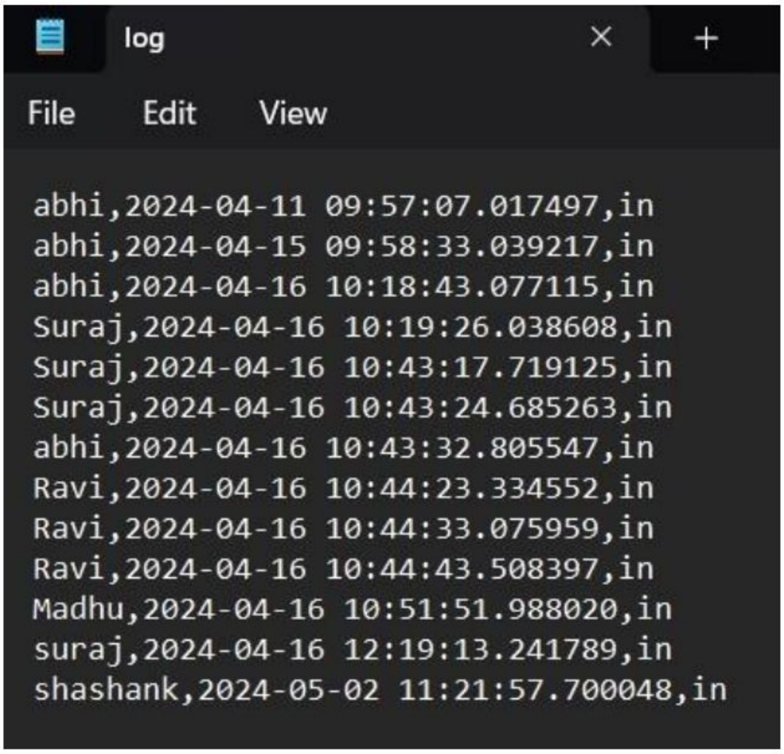


Welcome back !

Welcome, shashank.

Fig 7.1.4 Detection of visitor

After clicking upload image in web server the server will automatically predict the face by comparing the test set. Generated result will be the label and that should be the person name of that which is already there in database.



```
abhi,2024-04-11 09:57:07.017497,in
abhi,2024-04-15 09:58:33.039217,in
abhi,2024-04-16 10:18:43.077115,in
Suraj,2024-04-16 10:19:26.038608,in
Suraj,2024-04-16 10:43:17.719125,in
Suraj,2024-04-16 10:43:24.685263,in
abhi,2024-04-16 10:43:32.805547,in
Ravi,2024-04-16 10:44:23.334552,in
Ravi,2024-04-16 10:44:33.075959,in
Ravi,2024-04-16 10:44:43.508397,in
Madhu,2024-04-16 10:51:51.988020,in
suraj,2024-04-16 12:19:13.241789,in
shashank,2024-05-02 11:21:57.700048,in
```

Fig 7.1.5 log history of visitor

The history of the visitors will be recorded in log file. Where you access and look at each visitor visited at what time of both in and out. And the Date.

7.2 ACCURACY AND LOSS ANALYSIS

The analysis of a User Authentication System utilizing M-YOLOv4-C for face authentication involves evaluating various aspects of the system's performance, accuracy, security, and user experience. Measure the accuracy of face authentication by assessing the system's ability to correctly identify individuals.

Evaluate the detection speed to ensure real-time performance, which is crucial for practical applications. Consider the impact of factors such as lighting conditions, pose variations, and occlusions on accuracy. Understand the architecture of M- YOLOv4-C, including its deep learning components and how it contributes to accurate face recognition. Analyze the efficiency and computational requirements of the model, especially in resource constrained environments.

The accuracy rate of a visitor face authentication system using OpenCV depends on various factors, including the quality of the collected dataset, the effectiveness of preprocessing techniques, the robustness of the face recognition model, and the chosen threshold for similarity scores. Generally, face recognition systems can achieve high accuracy rates under controlled conditions with well-lit environments and cooperative subjects.

However, real-world scenarios may introduce challenges such as variations in lighting, occlusions, facial expressions, and changes in appearance over time. These factors can affect the system's accuracy and lead to false positives or false negatives.

Typically, accuracy rates for face recognition systems can range from 90% to 99% in ideal conditions. Achieving higher accuracy often requires continuous refinement of the system through dataset augmentation, model optimization, and fine-tuning of parameters.

Regular testing and evaluation are essential to measure the system's accuracy and identify areas for improvement. Additionally, monitoring the system's performance in production environments allows for adjustments to optimize accuracy over time.

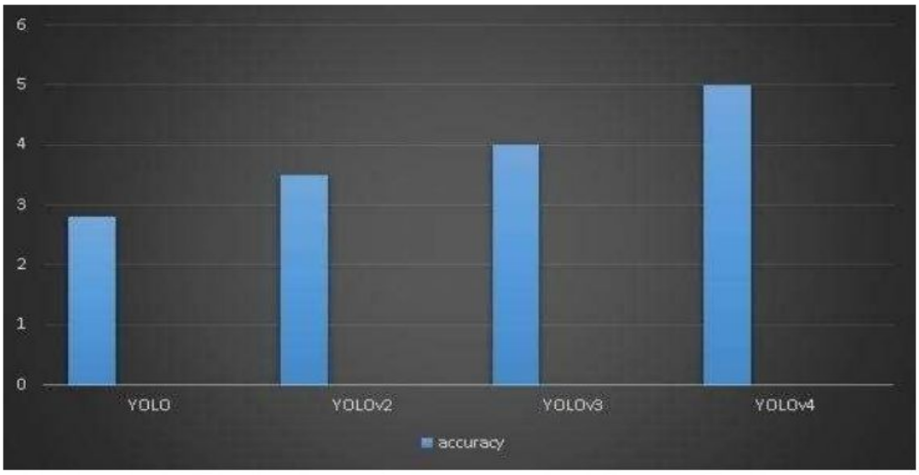


Fig 7.2.1 Accuracy rate of YOLO V4

From the above figure, Compare the performance of MYOLOv4-C with other face authentication methods, considering factors like accuracy, speed, and robustness. Evaluate how M-YOLOv4-C performs in comparison to traditional methods, such as Haar cascades or earlier versions of YOLO. Assess the system's robustness against potential security threats, including adversarial attacks and attempts at identity spoofing. Evaluate the effectiveness of any additional security measures, such as liveness detection, to ensure the presented face is from a live individual. Examine the efficiency of the database management system in storing and retrieving facial embeddings. Analyze the scalability of thesystem as the size of the user database grows.

CONCLUSION

CHAPTER 8

CONCLUSION

The substantial advancement of deep learning technology is covered in the paper, with special attention to image recognition with the M-YOLOv4-C model—a modification of the YOLO (You Only Look Once) architecture. Applications of deep learning include voice and image recognition, and it is now a key component of developing markets like autonomous vehicles and crime prevention monitoring systems.

A Closed-Circuit Television (CCTV) system employs the M-YOLOv4-C model to detect a visitor's face and identify 81 feature points in the face. Based on these features, a set of vector values is generated. A database contains the face images of family members who have pre-registered. The paper discusses the rapid advancement of deep learning technology, particularly in image recognition using the M-YOLOv4-C model, a variant of the YOLO (You Only Look Once) architecture. Deep learning has found applications in voice and image recognition, and it is now playing an important role in emerging industries such as autonomous driving and crime prevention monitoring systems.

The M-YOLOv4-C model is used in a Closed-Circuit Television (CCTV) system to detect a visitor's face and recognize 81 feature points in the face to generate a set of vector values based on The suggested model's evaluation metrics using M-YOLOv4-C are given. In particular, the inference time for Tiny-YOLOv3 is 6.5 FPS with an accuracy of 86.3%, and for YOLOv3, it is reported as 2.4 frames per second (FPS) with an accuracy of 90.3%.these features. Face images of pre-registered family members are saved in a database. The system is programmed to open the front door when a new visitor is identified as a family member. Future research, according to the paper, ought to concentrate on broadening the system's uses, like creating access control systems for stores or eateries. This would entail keeping track of visitors, storing visit records, automatically registering frequent visitors, and limiting access based on visitor recognition. Furthermore, there is a request for the creation of a face recognition-based access authentication system that uses the M-YOLOv4-C model's capabilities as a low-false detection rate substitute for passwords or fingerprints.

8.1 FUTURE ENHANCEMENT

Future enhancements for the face visitor authentication system could include:

1. Improved Accuracy and Speed: Continuously enhancing the M-YOLOv4-C model to improve accuracy and reduce inference time, enabling faster and more reliable face detection and recognition.
2. Expansion of Feature Points: Expanding the number of feature points detected in the face to capture more detailed facial characteristics, improving the accuracy of face recognition.
3. Database Management Enhancements: Developing more robust database management capabilities to handle larger datasets, store visit records, and automatically register frequent visitors for quicker authentication.
4. Access Control System Integration: Integrating the authentication system with access control systems for stores or eateries, enabling visitor tracking, automated registration, and access restriction based on recognition.
5. Alternative Authentication Methods: Exploring the use of the M-YOLOv4-C model for alternative authentication methods such as replacing passwords or fingerprints with facial recognition, leveraging its low false detection rate.
6. Real-Time Monitoring and Alerts: Implementing real-time monitoring and alerting features to notify administrators of any security breaches or suspicious activities detected by the authentication system.
7. Adaptation to New Environments: Adapting the system to function effectively in different environments and lighting conditions, ensuring reliable performance in various settings.
8. Integration with IoT Devices: Integrating the authentication system with Internet of Things (IoT) devices for enhanced automation and connectivity, allowing seamless integration with smart home or building systems.aster processing of user requests and to get quick result.

REFERENCES

REFERENCES

[1]. Y. Indulkar, "Alleviation of COVID by means of Social Distancing & Face Mask Detection Using YOLO V4," 2021 International Conference on Communication information and Computing Technology (ICCICT), Mumbai, India, 2021, pp. 1-8, doi: 10.1109/ICCICT50803.2021.9510168.

[2]. Y. Indulkar, " Visitor Authentication Based & Face Mask Detection Using YOLO V4," 2020 International Conference and Computing Technology (ICCICT), Mumbai, India, 2021, pp. 1-8, doi: 10.1109/ICCICT50803.2021.9510168.

[3]. Howard A, Sandler M, Chen B, Wang W, et al. Searching for MobileNetV3. In: 2019 IEEE/CVF International Conference on Computer Vision (ICCV). Seoul, Korea(South); 2019. p. 1314- 24.

[4]. H. -J. Mun and M. -H. Lee, "Design for Visitor Authentication Based on Face Recognition Technology Using CCTV," in IEEE Access, vol. 10, pp. 124604-124618, 2022, doi: 10.1109/ACCESS.2022.3223374.

[5]. T. A. Kiran, N. D. K. Reddy, A. I. Ninan, P. Krishnan, D. J. Aravindhar and A. Geetha, "PCA based Facial Recognition for Attendance System," 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2020, pp. 248-252, doi: 10.1109/ICOSEC49089.2020.9215326.

[6]. J. Zheng, J. Zheng, S. Zhang, H. Yu, L. Kong and D. Zhigang, "Segmentation Method for Whole Vehicle Wood Detection Based on Improved YOLACT Instance Segmentation Model," in IEEE Access, vol. 11, pp. 81434-81448, 2023, doi: 10.1109/ACCESS.2023.3300900.

[7]. A. Boragule, K. C. Yow and M. Jeon, "On-device Face Authentication System for ATMs and Privacy Preservation," 2023 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2023, pp. 1-4, doi: 10.1109/ICCE56470.2023.10043387.

[8]. M. Luo, J. Cao, X. Ma, X. Zhang and R. He, "FA-GAN: Face Augmentation GAN for Deformation-Invariant Face Recognition," in IEEE Transactions on Information Forensics and Security, vol. 16, pp. 2341-2355, 2021, doi: 10.1109/TIFS.2021.3053460.

[9]. Alzu‘bi, A.; Albalas, F.; AL-Hadhrami, T.; Younis, L.B.; Bashayreh, A. Masked Face Recognition Using Deep Learning: A Review. Electronics 2021, 10, 2666.

[10]. R. He, X. Wu, Z. Sun, and T. Tan, ―Learning invariant deep representation for NIR-VIS face recognition,‖ in Proc. 31st AAAI Conf. Artif. Intell., 2017,pp. 2020-2021.

[11] R. He, X. Wu, Z. Sun, and T. Tan, ―Wasserstein CNN: Learning invariant features for NIR-VIS face recognition,‖ IEEE Trans. Pattern Anal. Mach. Intell., vol. 41, no. 7, pp. 1761–1773, Jul. 2019.

[12] X. Di, B. S. Riggan, S. Hu, N. Short, and V. Patel, ―Polarimetric thermal to visible face verification via self-attention guided synthesis,‖ in Proc. Int. Conf. Biometrics, 2019, pp. 1–8.

[13]. K. Yu, G. Tang, W. Chen, S. Hu, Y. Li and H. Gong, "MobileNet-YOLO v5s: An Improved Lightweight Method for Real-Time Detection of Sugarcane Stem Nodes in Complex Natural Environments," in IEEE Access, vol. 11, pp. 104070-104083, 2023, doi: 10.1109/ACCESS.2023.3317951.

[14]. L. L. Chambino, J. S. Silva, and A. Bernardino, ‗‗Multispectral facial recognition: A review,'' IEEE Access, vol. 8, pp. 207871– 207883, 2020, doi: 10.1109/ACCESS.2020.3037451.

[15] K. Kim, B. Lee, and J. W. Kim, ‗‗Feasibility of deep learning algorithms for binary classification problems,'' J. Intell. Inf. Syst., vol. 23, no. 1,pp. 95–108, Mar. 2017, doi: 10.13088/jiis.2017.23.1.095.

[16] R. Girshick, J. Donahue, T. Darrell, and J. Malik, ‗‗Rich feature hierarchiesfor accurate object detection and semantic segmentation,'' in Proc. IEEEConf. Comput. Vis. Pattern Recognit., Jun. 2014, pp. 580–587.

[17] A. Kumari Sirivarshitha, K. Sravani, K. S. Priya and V. Bhavani, "An approach for Face Detection and Face Recognition using OpenCV and Face Recognition Libraries in Python," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), Coimbatore, India, 2023, pp. 1274-1278, doi: 10.1109/ICACCS57279.2023.10113066.

[18] S. Ren, K. He, R. Girshick, and J. Sun, ‗‗Faster R-CNN: Towards real time object detection with region proposal networks,'' IEEE Trans. PatternAnal. Mach. Intell., vol. 39, no. 6, pp. 1137–1149, Jun. 2016.

[19]. P. Mary Jenifer, P. Mahasri, A. Omsai, B. I. Humaira and R. Dhnaalakshmi, "Multiple Face Detection and Attendance System Using OpenCV," 2021 International Conference on Simulation, Automation & Smart Manufacturing (SASM), Mathura, India, 2021, pp. 1-5, doi: 10.1109/SASM51857.2021.9841223.

[20] W. Fang, L. Wang, and P. Ren, ‗‗TinierYOLO: A real-time object detection method for constrained environments,'' IEEE Access, vol. 8,pp. 1935–1944, 2020, doi: 10.1109 /ACCESS.2019.2961959.

[21] K. M. Lee, H. Song, J. W. Kim, and C. H. Lin, __Balanced performancefor efficient small object detection YOLOv3-tiny,'' in Proc. Korean Soc.Broadcast Eng. Conf. Anseong, South Korea: The Korean Institute ofBroadcast and Media Engineers, Nov. 2018, pp. 117–118

[22]. Pedoeem J, Huang R, Chen C. YOLO-LITE: A real-time object fetection algorithm optimized for non-GPU computers. In: 2018 IEEE International Conference on Big Data (Big Data). Seattle, WA, USA; 2018. p. 2503-10.

[23]. Bochkovskiy A, Wang CY, Liao HYM. YOLOv4: Optimal speed and accuracy of object detection. arXiv preprint; 2020: arXiv:2004.10934.

[24] Howard A, Sandler M, Chen B, Wang W, et al. Searching for MobileNetV3. In: 2019 IEEE/CVF International Conference onComputer Vision (ICCV). Seoul, Korea(South); 2019. p. 1314-24

[25]. Wang K, Chen C, He Y. Research on pig face recognition model based on keras convolutional neural network. In: Proceeding of the 2nd International Conference on Environmental Prevention and Pollution Control Technologies (EPPCT2020). Sanya, Hainan, China; 2020. p. 411-20

[26]. M. Alsawwaf, Z. Chaczko, M. Kulbacki, and N. Sarathy, __In your face:Person identification through ratios and distances between facial features,''Vietnam J. Comput. Sci., vol. 9, no. 2, pp. 187–202, May 2022, doi: 10.1142/S2196888822500105

[27] S. Han, __Age estimation from face images based on deep learning,'' inProc. Int. Conf. Comput. Data Sci. (CDS), Stanford, CA, USA, Aug. 2020,pp. 288–292, doi: 10.1109/CDS49703.2020.00063.

[28] Q. Guo, Z. Wang, C. Wang, and D. Cui, __Multi-face detection algo rithm suitable for video surveillance,'' in Proc. Int. Conf. Comput. Vis.,Image Deep Learn. (CVIDL), Chongqing, China, Jul. 2020, pp. 27–33, doi:10.1109/CVIDL51233.2020.00013.

[29] M. Waseem, S. A. Khowaja, R. K. Ayyasamy, and F. Bashir, __Facerecognition for smart door lock system using hierarchical network,'' inProc. Int. Conf. Comput. Intell. (ICCI), Seri Iskandar, Malaysia, Oct. 2020,pp. 51–56, doi: 10.1109/ICCI51257.2020.9247836.

[30] H.-J. Mun and K.-H. Han, __Design for access control systembased on voice recognition for infectious disease prevention,''J. Korea Converg. Soc., vol. 11, no. 7, pp. 19–24, Jul. 2020, doi:10.15207/JKCS.2020.11.7.019.

[31]. Bimantoro MZ, Emanuel AWR. Sheep Face Classification using Convolutional Neural Network. In: 2021 3rd East Indonesia Conference on Computer and Information Technology (EIConCIT). Surabaya, Indonesia; 2021. p. 111 Simulation, Automation & Smart

Manufacturing (SASM), Mathura, India, 2021, pp. 1-5, doi: 10.1109/SASM51857.2021.9841223.

[22] W. Fang, L. Wang, and P. Ren, __TinierYOLO: A real-time object detection method for constrained environments,'' IEEE Access, vol. 8,pp. 1935–1944, 2020, doi: 10.1109/ACCESS.2019.2961959.

[23] K. M. Lee, H. Song, J. W. Kim, and C. H. Lin, __Balanced performancefor efficient small object detection YOLOv3-tiny,'' in Proc. Korean Soc.Broadcast Eng. Conf. Anseong, South Korea: The Korean Institute ofBroadcast and Media Engineers, Nov. 2018, pp. 117–118

[22]. Pedoeem J, Huang R, Chen C. YOLO-LITE: A real-time object fetection algorithm optimized for non-GPU computers. In: 2018 IEEE International Conference on Big Data (Big Data). Seattle, WA, USA; 2018. p. 2503-10.

[23]. Bochkovskiy A, Wang CY, Liao HYM. YOLOv4: Optimal speed and accuracy of object detection. arXiv preprint; 2020: arXiv:2004.10934.

[24] Howard A, Sandler M, Chen B, Wang W, et al. Searching for MobileNetV3. In: 2019 IEEE/CVF International Conference onComputer Vision (ICCV). Seoul, Korea(South); 2019. p. 1314-24

[25]. Wang K, Chen C, He Y. Research on pig face recognition model based on keras convolutional neural network. In: Proceeding of the 2nd International Conference on Environmental Prevention and Pollution Control Technologies (EPPCT2020). Sanya, Hainan, China; 2020. p. 411-20

[26]. M. Alsawwaf, Z. Chaczko, M. Kulbacki, and N. Sarathy, __In your face:Person identification through ratios and distances between facial features,''Vietnam J. Comput. Sci., vol. 9, no. 2, pp. 187–202, May 2022, doi: 10.1142/S2196888822500105

[31] S. Han, __Age estimation from face images based on deep learning,'' inProc. Int. Conf. Comput. Data Sci. (CDS), Stanford, CA, USA, Aug. 2020,pp. 288–292, doi: 10.1109/CDS49703.2020.00063.

[32] Q. Guo, Z. Wang, C. Wang, and D. Cui, __Multi-face detection algo rithm suitable for video surveillance,'' in Proc. Int. Conf. Comput. Vis.,Image Deep Learn. (CVIDL), Chongqing, China, Jul. 2020, pp. 27–33, doi:10.1109/CVIDL51233.2020.00013.

VISITOR FACE AUTHENTICATION USING DEEP LEARNING

Dr. Pradeep V[1,a] , Likhita k m[2,b] , Ravindra Reddy[2,c] , Shashank Biradar[2,d] , Suraj Ankolekar[2,e]

[1]Associate Professor, [2]B.E. Students
Departmentof Information Science and Engineering
Alva's Institute of Engineering and Technology Mangalore, India

[a]writetopv@gmail.com , [b]likhitagwoda@gmail.com , [c]ravindrareddykothakapu@gmail.com ,
[d]shashanksatishkumar10@gmail.com , [e]surajankolekar9@gmail.com

ABSTRACTION: Deep learning-based image recognition technology has advanced recently, and home services and security systems that use biometric data like fingerprints, iris scans, and facial recognitionare gaining popularity. Specifically, a great deal of research has been done on face recognition- based user authentication techniques. With the goal of improving human face detection, this study suggests a brandnew model called MobileNetv3- YOLOv4-PACNet (M-YOLOv4-C). The main goal is to increase the effectiveness of distinguishing distinct faces in a range of situations. The goal is to overcome the limitations of traditional face detection techniques by utilizing a novel, non-invasive method. The lightweight MobileNet-v3 network is used in placeof the original YOLOv4 backbone in the proposed model, and depth-wise separable convolution is included to simplify the network parameters. The goal of integrating CAM and SAM into a CBAM attention mechanism is to maintain high accuracy while reducing the sizeof the model. Important facial features are selectively strengthened while less relevant information is filtered out by the innovative multi-attention mechanism. The model performs admirably, yielding a mean Average.

Introduction

The emphasis on "scientific, systematic, and intelligent cultivation" in the context of human management provides a segue into discussing advanced technologies in human face authentication. The growing importance of ensuring effective and secure management practices aligns with the broader trend of enhancing security measures in various domains, including human identity verification.

In the realm of human face authentication, technological advancements have indeed progressed significantly in recent years. Face recognition systems, powered by deep learning and artificial intelligence, have become integral for security access control [1], and user authentication. The increasing need for robust and reliable identification methods parallels the importance of security highlighted in the initial passage.

Just as the passage underscores the importance of technological solutions for accurate detection and identification in face, face authentication technologies leverage sophisticated algorithms to accurately identify and verify individuals based on their facial features. These technologies play a crucial role in various sectors [2], including cybersecurity, law enforcement, and secure access control systems. The passage's reference to "benign guarantee" in security aligns with the ethical considerations and user privacy concerns associated with human face authentication. As technologies advance, ensuring the responsible and ethical use of face recognition becomes paramount.

Precise and timely identification of persons is critical, particularly in the context of facial recognition. By using cutting-edge technologies to accurately identify faces [3],[4]. people can be watched over and promptly intervened upon exhibiting odd behaviors or posing a security risk. Maintaining a secure environment and lowering the risk of incidents require this proactive eapproach [5],[6].

Human face detection technology is useful for a variety of purposes outside of security, such as fraud prevention. By verifying people's identities, technology aids in the prevention of fraudulent activities in industries like identity verification and insurance. This promotes a win-win relationship between people and institutions while also providing protection against malicious activity.

In the context of human face detection, the idea of win-win cooperation is still relevant. Through the use of this technology, institutions and individuals alike can benefit. People gain from improved security and fraud protection, and organizations like insurance companies can maintain integrity and expedite procedures. The methodical incorporation of facial recognition technology advances the general security and identity standards by supporting dependable and effective management practices across a range of industries. The tremendous progress made inface recognition technology can be attributed in large part to the effective integration of Deep Learning (DL), especially when it comes to the recognition of human faces. A number of novel techniques and models have been presented, indicating the advancement of face recognition technology. The HRPSM_CNN approach was presented by Tamilselvi et al. [7],[8], who also provided evidence of its accuracy and efficacy in face recognition in a variety of settings. In the LFW face database, this method's accuracy of 96% was quite impressive. With the integration of the SE module into Mobile Face Net, Liu et al. [9],[10],[11] achieved an exceptional accuracy of 99.67% in the LFW dataset. This accomplishment is noteworthy because it highlights efficiency gains with smaller model parameters and a smaller storage footprint of just 5.36 MB [12],[13].

The benefits of DL have been utilized in the current application of non-contact automatic identification technology. Deep learning for facial recognition holds great potential in a range of fields, including identity verification, access control, and security [14],[15],[16].

Diverse CNN models have been presented by researchers to recognize faces of pigs, demonstrating ongoing efforts to increase accuracy. A CNN model based on LeNet-5 was created by Wang et al. [17],[18],[19] and achieved an astounding 97.6% accuracy. By combining data from several layers to create the final individual identity feature, Qin et al. [20] used the Bilinear CNN and were able to achieve a 95.73% recognition accuracy. Furthermore, two cascade classifiers based on Haar features and a shallow CNN were used by Mathieu et al. [21] for face and eye tracking, in addition to a deep CNN for pig face recognition. By adding a marginal loss function based on triples, Wang et al. [22] enhanced many CNN models and achieved 96.8% recognition accuracy across 28 pigs. Wang and colleagues [23] improved the multiscale network architecture.

Previous research has demonstrated significant progress in addressing generalization and accuracy issues in applications pertaining to facial recognition [24],[25], which is consistent with the current trend toward production systems that are lightweight, economical, and highly generalized [26],[27],[28].

A primary focus is on optimizing models to minimize administrative expenses, increase speed, and decrease computing needs while preserving high accuracy. The work takes advantage of the one stage YOLO-v4 algorithm's many practical applications and uses its features to inform algorithm design [29]. More specifically, improving channel and geographical information and optimizing the feature extraction procedure are prioritized.

The suggested method, known as the M-YOLOv4-C network [30],[31], is intended to investigate the identification of multiple individuals in human faces and is based on YOLO-v4 as the baseline.

Related work:

User Authentication:

User authentication using the MYOLOv4-C model for face recognition represents a sophisticated and efficient approach to secure access control systems. In a world increasingly reliant on biometric technologies, this system leverages the power of the M-YOLOv4- C model to ensure reliable and accurate identification of individuals based on their facial features [18],[19]. The first crucial step in this authentication process is the collection of input data. Facial images of users are captured using cameras or other imaging devices, ensuring that the images are high-quality and capture the unique facial characteristics necessary for accurate recognition. Preprocessing of these images follows, involving normalization and resizing to match the input dimensions expected by the MYOLOv4-C model [20],[21],[22].

Integration of the pre-trained M-YOLOv4-C model is a pivotal aspect. This model, known for its one-stage object detection capabilities, becomes the cornerstone of the facial recognition system. It excelsin detecting objects, in this case, human faces, and extracting relevant features [23],[24].As the model processes facial images, it extracts features that form a unique representation of each user's face [25],[26]. During the user enrollment phase, these features are stored, associating each user with a unique identifier linked to their facial representation. This enrollment phase iscritical for establishing a baseline for future authentication attempts.

The authentication process itself involves capturing the facial image of a user attempting to gain access [27]. This image is then processed through the MYOLOv4-C model for feature extraction. The extracted features are compared to the stored features of enrolled users using amatching algorithm [28],[29]. If a match is found, the user is authenticated, and access is granted. Conversely, if no match is found, access is denied, and the attempt may be logged forfurther analysis. To enhance system robustness, continuous learning mechanisms can be implemented. These mechanisms adapt the model to changes in users' appearances over time, ensuring the system remains accurate and effective in dynamic environments. Regular updates to the enrolled userdatabase with new facial features contribute to this adaptability. Security measures are paramount in any authentication system. Liveness detection, which verifies that the presented face is from a live person and not a static image or video, helps prevent spoofing attacks [30].

Additionally, encryption and secure storage of facial feature representations protect against unauthorized access and data breaches.Logging and monitoringare integral components of a comprehensive authentication system. Logging authentication attempts provides an audit trail for security analysis, helping identify and address potential threats. Continuous monitoring of the system's performance and accuracy over time ensures itsongoing effectiveness. user authentication using the M-YOLOv4-C model for face recognition combines cutting-edge technology with robust security measures. This approach addresses thechallenges of generalization and accuracy, offering a lightweight [31], cost-effective, and highly generalized solution. By integrating state-of-the-art object detection capabilities with continuous learning mechanisms and stringent security measures, this authentication system stands as a reliable and efficient method for securing access to sensitive areas and information.

Ownership-based authentication

Using deep learning and powerful object detection, ownership-based authentication with M- YOLOv4-C verifies users based on who owns a certain physical object. The first step in the procedure is choosing unique things that users will present for verification, including ID cards, personal devices, or certain items. The model is trained to identify and categorize these ownedthings using M-YOLOv4-C, which is renowned for its strong object detection abilities. Images of users displaying their owned property are taken during user enrollment, and ownership features are retrieved and safely kept. When a user presents their object during the authentication process, M-YOLOv4-C recognizes it, classes it, and extracts ownership features for confirmation. When these features match data that has been stored, the system grants access.

Multi-factor authentication

MFA begins with the selection of distinct authentication factors, typically categorized as something the user knows (e.g., password), something the user has (e.g., owned object), and something the user is (e.g., facial features). M-YOLOv4-C, renowned for precise object detection, is chosen as the base model for recognizing and classifying owned objects. During user enrollment, the system captures various factors: facial features, ownership of a unique object, and potentially a password. M-YOLOv4-C processes images, extracting features and ensuring ownership verification. Additionally, the model adapts to facial features for user recognition.

In the authentication process, users present their owned objects, and the system employs M- YOLOv4-C to detect and classify the object. Simultaneously, facial recognition technology verifies the user's identity. The password may serve as an additional factor. Access is granted only when all factors align, providing a multi-layered and secure authentication process.This MFA approach enhances security by requiring attackers to compromise multiple factors, significantly reducing the risk of unauthorized access. Continuous learning mechanisms and robust encryption further fortify the system. Logging and monitoring track authentication attempts, ensuring ongoing security evaluation.

MFA using M-YOLOv4-C not only leverages advanced object detection for ownership verification but also integrates facial recognition and potentially other factors, creating a comprehensive and resilient authentication system.

Object characteristic-based authentication

The process starts with the users' unique possessions or personal devices that have been carefully chosen. The M- YOLOv4-C model, which is renowned for its accurate object detection skills, is utilized to train the model to identify and categorize these objects accordingto their distinct attributes.

Images of users displaying their owned objects are taken by the system during user enrolmentand M-YOLOv4-C processes these images to extract and safely store the objects' distinguishingfeatures. These characteristics act as an individual fingerprint for every object. Users present their owned objects during the authentication process, and M-YOLOv4-C is used to identify and categorize the object based on its attributes. After that, the system .

MATERIALS AND METHODS

Similar to a pig farm, the data were collected from people in a particular area, and a portable smartphone was used to take a picture of each person's face. As with the pig study, the objectivewas to guarantee data continuity and reliability. A conscious effort was made to take pictures of a single person facing the camera from different perspectives during the collection process. This strategy aims to improve a later model's capacity for generalization, reflecting the pig study's consideration of various viewpoints.

Similar to the pig study, the subjects' faces weren't cleaned before the photos were taken. In order to increase variability in the dataset and facilitate the extraction of a more varied set of facial features, this decision was made. This choice was made in order to extract a wider range of facial features, which will increase dataset variability and allow the model to adjust to a variety of facial appearances. It's crucial to stress that rigorous ethical guidelines must be followed in any study involving human subjects. These guidelines include getting participants' informed consent and making sure participant privacy and confidentiality are protected. Research involving human facial data requires careful attention to ethical issues and relevant regulatory compliance.

Introduce to YOLOv4 algorithm:

The four components of the YOLOv4 [29] model are the head network of YOLOv3, the feature fusion module of Neck (PANet), the additional module of Neck (SPP), and the backbone network (CSP-Darknet53). Darknet53 has been enhanced by the CSP Net-based backbone network CSPDarknet-53 to lessen gradient disappearance. On the other hand, the network has a higher input resolution, more network layers, and a significantly higher number of parameters.

The receptive field is greatly expanded by the SPP addition module, and PANet is utilized for parameter aggregation in place of FPN to accommodate varying degrees of object detection. The YOLOv3 detection head is still utilized in the detection head section to perform.

Introduce to MobileNet-v3 algorithm:

The Google-proposed MobileNet-v3 is a lightweight model network. In this version, linear bottleneck, inverted residuals, depth-wise separable convolution, and The H-Swish function and SE module increase the accuracy of the original Mobile Net series. The B neck section within the MobileNet-v3 network is displayed. The input starts off via 1 × 1 conventional convolution and 3 × 3 depth- wise input into the SE attention module following separable convolution. It is multiplied after the Pool and FC layers activate it. with the initial input and then added with the input at the end to obtain the output feature map.

The network structure of MYOLOv4-C network:

The goal of this study was to investigate a better algorithm for pig face recognition, and to that end, the MYOLOv4-C network was built. This network chose MobileNet-v3 as its backbone network because it can drastically cut down on computation and parameters while also increasing running speed. Furthermore, to carry out the lightweight experiments, depth-wise separable convolution was used in place of the common convolution in SPP and PANet. Additionally, the CBAM module was added to PANet's up sampling process in order to increase accuracy by concatenating channels and space. The Loss function employed was the CIOU Loss.

Backbone network structure

The structure of the backbone network is shown (1) The first column Input represents the scaleof input feature layer, and the outputs of the 8th, 14th and 16th layers are respectively used as out1, out2, and out3 in the incoming enhanced feature extraction network; (2) The second column Operator represents the type and size of convolution kernel; (3) The third column Nonlinearitie represents the type of activation function used; (4) The fourth column SE is used to indicate whether this layer of network has introduced the Squeeze and Excitation (SE) attentionmechanism; (5) The fifth column Stride represents the stride of each convolution. If the strideis 2, the width and height of the next feature layer will be half of the previous feature layer.

SPP structure

The full name of SPP is Spatial Pyramid Pooling. The purpose in this network is to expand thereceptive field of feature maps. The implementation is to carry out depth-wise separable convolution on the output of backbone network, and then perform the maximum pooling of5 x5,9 9, x13 x 13 respectively, and finally concatenate them into PANet.

ACCESS CONTROL SYSTEM

The Access Control System utilizing MYOLOv4-C for face authentication represents a state- of-the-art solution at the intersection of advanced computer vision and access management technologies. This system is meticulously designed to provide secure and efficient access control, leveraging the capabilities of M-YOLOv4-C, a powerful object detection and classification model.

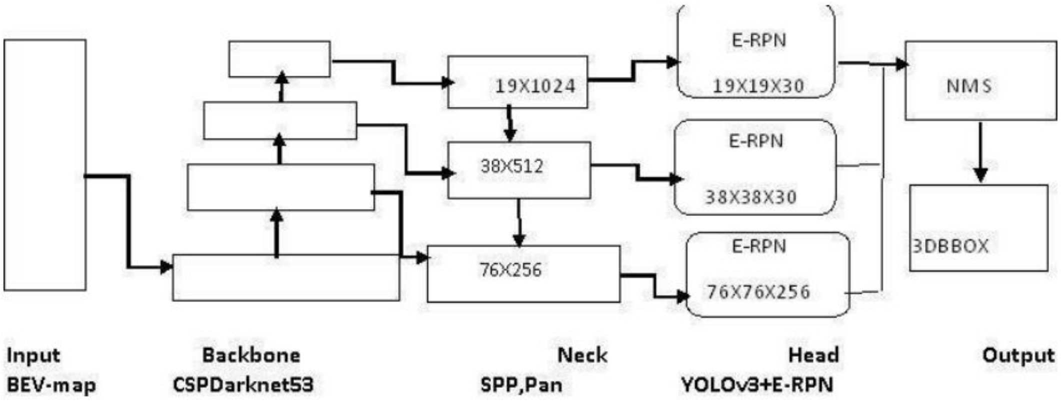


Figure 1: Yolo v4 Networking holistic framework

Enrollment Process:

In the initial phase, users are enrolled in the system by capturing images of their faces using a handheld smartphone or dedicated cameras equipped with MYOLOv4-C. This process is crucial for creating a comprehensive database of facial features. M-YOLOv4-C processes these images, extracting and securely storing facial features that serve as unique identifiers for each individual.

Authentication Process:

During the authentication process, users present their faces for verification. MYOLOv4-C is employed to detect and classify facial features in real-time. The model's robust object detection capabilities ensure accurate identification, even in challenging scenarios such as varying lighting conditions or different facial angles.

Multi-Factor Authentication (Optional):

For enhanced security, the system has the flexibility to integrate multi-factor authentication. This can include additional factors such as the ownership of a unique object or the input of a password. Multi-factor authentication adds an extra layer of protection, making it more challenging for unauthorized individuals to gain access.

Continuous Learning Mechanisms:

To adapt to changes in facial appearances over time, the system incorporates continuous learning mechanisms. This ensures that the model remains effective in recognizing faces, even as individuals undergo natural changes in their appearances. Continuous learning contributes to the system's adaptability and long-term reliability.

Liveness Detection:

To prevent potential spoofing attempts, liveness detection measures are implemented. This functionality ensures that the presented face is from a live individual, adding an additional layerof security against unauthorized access through the use of photographs or other non-living representations.

Logging and Monitoring:

The system maintains a comprehensive log of authentication attempts, including successful and unsuccessful events. This log is instrumental in monitoring the system's performance, identifying potential security threats, and conducting post-event analysis. Realtime monitoring allows for swift responses to any anomalies or suspicious activities.

Advantages of the System:

M-YOLOv4-C, with its advanced object detection, provides a high level of accuracy in facial feature recognition. Security: Multi-factor authentication, liveness detection, and continuous learning mechanisms contribute to a robust security framework.

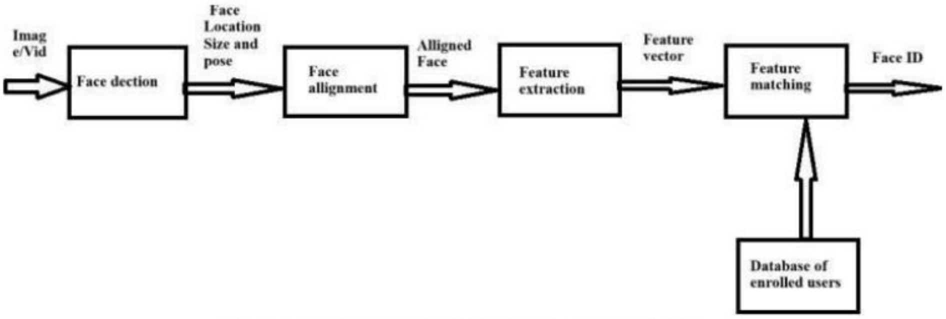
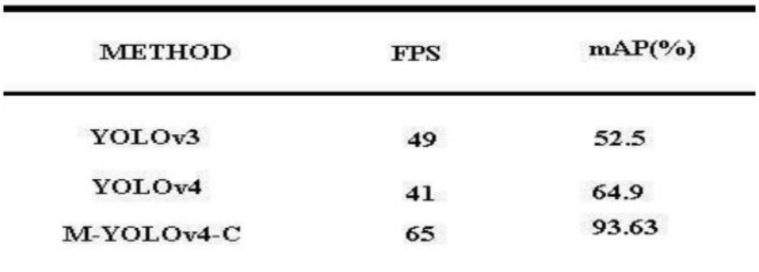


Figure 2: Access control using a smart mirror.

The system offers a seamless and user-friendly experience, requiring only the presentation of the face for quick and secure access. Adaptability: Continuous learning ensures the model adapts to variations in facial appearances, maintaining effectiveness over time.

Efficiency:

Real-time processing capabilities of M-YOLOv4-C contribute to swift and efficient face authentication, facilitating seamless access control. The Access Control System utilizing MYOLOv4-C for face authentication represents a state-of-the-art solution at the intersection of advanced computer vision and access management technologies. This system is meticulously designed to provide secure and efficient access control, leveraging the capabilities of M-YOLOv4-C, a powerful object detection and classification model.



METHOD	FPS	mAP(%)
YOLOv3	49	52.5
YOLOv4	41	64.9
M-YOLOv4-C	65	93.63

Table 1: Efficiency of Yolo v4 Algorithm

The backbone architecture of YOLO v4, often based on Darknet, efficiently extracts features from input images, contributing to accurate predictions. The utilization of anchor boxes helps the model focus on predicting bounding boxes more precisely. YOLO v4 introduces architectural improvements and optimizations over its predecessors, enhancing overall performance and efficiency.

The efficiency of the YOLO v4 (You Only Look Once version 4) algorithm stems from its design principles, making it well-suited for real-time object detection tasks. YOLO v4 processes images in real-time, crucial for applications such as video analysis and surveillance. Its strength lies in conducting object detection in a single forward pass, avoiding the need for multiple passes through the neural network.

STRUCTURE AND PROTOCOL OF THE PROPOSED SYSTEM

USER AUTHENTICATION SYSTEM:

The integration of MariaDB on the Jetson Nano for the establishment of a visitor access control database signifies a sophisticated approach to managing and storing crucial access-related information.

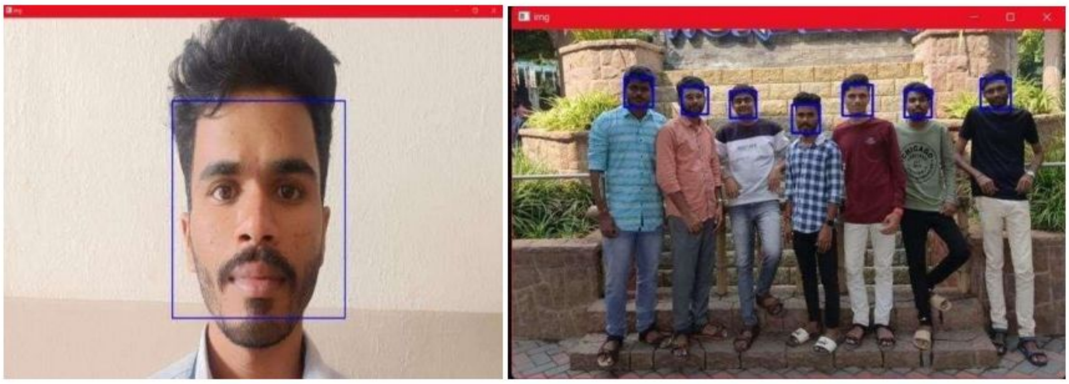


Figure 3: Facial Recognition with Deep Learning

A Facial Recognition Pipeline with Deep Learning represents a comprehensive approach to automating the identification of individuals based on their facial features .A user authentication system verifies user identity for access, typically using passwords, biometrics, or multi-factor methods. Security measures include encryption and regular updates. Prioritizing privacy and adhering to industry standards, modern systems often integrate advanced technologies for enhanced protection against unauthorized access. This sophisticated system integrates various stages, each playing a crucial role in achieving accurate and efficient facial recognition.

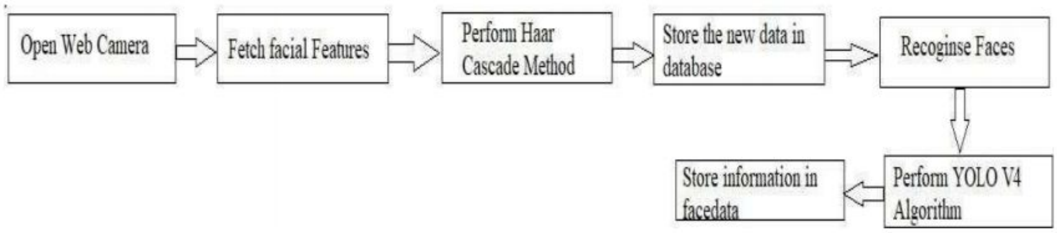

Open Web Camera
Fetch facial Features
Perform Haar Cascade Method
Store the new data in database
Recoginse Faces
Perform YOLO V4 Algorithm
Store information in facedata

Figure 4: Registration Phases

Fisher Faces method worked great at least for the constrained scenario we've assumed in our model. In order to save the discriminative data, the Linear Discriminant. Analysis is used.

Data Collection:

The process begins with the acquisition of facial data. This can involve capturing images or video frames containing faces. Datasets are essential for training deep learning models, ensuring they learn diverse facial characteristics.

Data Preprocessing:

Raw facial images undergo preprocessing to enhance quality and prepare them for subsequent stages. Normalization, resizing, and grayscale conversion contribute to uniformity in the dataset, leading to improved

Step	**Action**	**Observation**
Image Capture	Connects with the installed camera and starts authenticating	Camera Started
Image file Loading	Loads the Haar Classifier Cascade files for the frontal face	Ready for Capturing
Face Location	Initiates the Face and Fetching the Frame work.	Image file has been extracted
Face Encoding	Initiating the YOLO V4 Algorithm for encoding the image file	Update the face data
Processing the face	It recognize and verifies the input face with the saved faces.	Nearest face Recognized

Table 2: Actions and Observations

Face Detection:

Face detection is a pivotal step in locating and identifying faces within images or video frames. Techniques such as Haar cascades or deep learning based methods, including Single Shot Multi box Detector (SSD) and MTCNN, are commonly employed for accurate and efficient face detection.

Face Alignment:

Post-detection, face alignment corrects variations in head pose and aligns facial features to a standardized position. This step ensures consistency in feature extraction, irrespective of different facial orientations.

Feature Extraction:

Feature extraction involves capturing discriminative features from facial images. Deep learning models, particularly Convolutional Neural Networks (CNNs), are widely used for this purpose. The objective is to represent facial characteristics in a way conducive to effective recognition.

Embedding Generation:

Extracted features are transformed into embeddings, compact representations encoding essential facial information. Models like Face Net or Open Face are popular for generating embeddings that capture unique facial signatures.

Database Storage:

The facial embeddings are stored in a database, associating each embedding with a unique identifier linked to the corresponding individual. This database serves as a reference for later recognition tasks.

Recognition:

During the recognition phase, facial embeddings of new or unseen faces are compared to stored embeddings in the database. Techniques like cosine similarity or Euclidean distance measurement are applied to determine the similarity between embeddings, facilitating identification or verification. The recognition phase in facial recognition involves detecting faces, extracting key features, and matching them against a database. Facial features are compared using similarity scores, and a threshold determines successful recognition. In visitor authentication, this phase identifies individuals based on pre-registered facial features, granting access if a match surpasses the threshold. Ethical considerations, privacy measures, and compliance with regulations are integral aspects in deploying facial recognition systems for secure and responsible use.

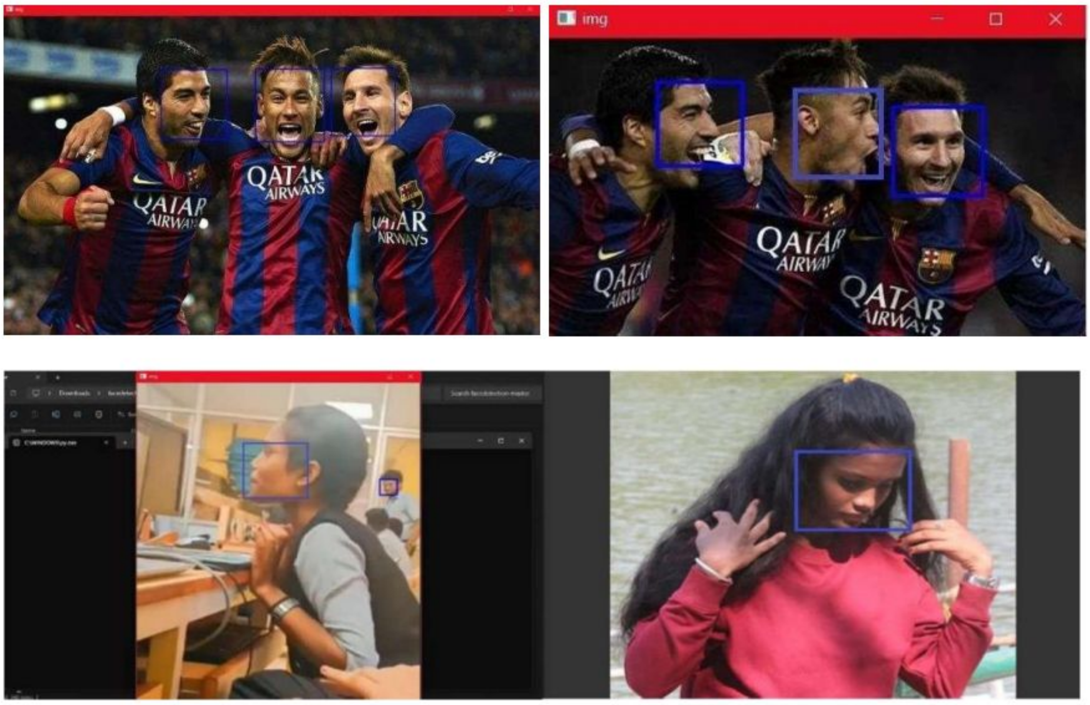


Figure 5: identification and unidentification of face while detecting

Decision/Output:

Based on the similarity measurement, a decision is made regarding the identity of the individual. This decision might involve classifying the face against known identities or verifying whether the face belongs to a particular person.

User Interface/Integration:

Create a user-friendly interface for visitor face authentication, ensuring a smooth registration process and clear feedback during authentication. Develop robust integration through well- documented APIs and compatibility with existing systems, prioritizing security, scalability, and compliance with data protection regulations. Enable customization options to align with organizational branding and aesthetics. Implement liveness detection prompts for added security. Provide comprehensive documentation and training resources for administrators. Regularly update the system to address security vulnerabilities and ensure optimal performance. This approach ensures a seamless, secure, and user-centric experience while seamlessly integrating with existing infrastructure.

The results of facial recognition can be presented through a user interface, integrated with access control systems, or applied to various applications such as attendance tracking, securitysystems, or personalized user experiences.

Continuous Learning (Optional):

Some facial recognition systems incorporate continuous learning mechanisms to adapt to changes in facial appearances over time. This ensures the model remains effective and accurate, especially in dynamic environments.

Security Measures:

To enhance security, additional measures such as liveness detection can be integrated to ensure that the detected face is from a live individual, preventing spoofing attempts.

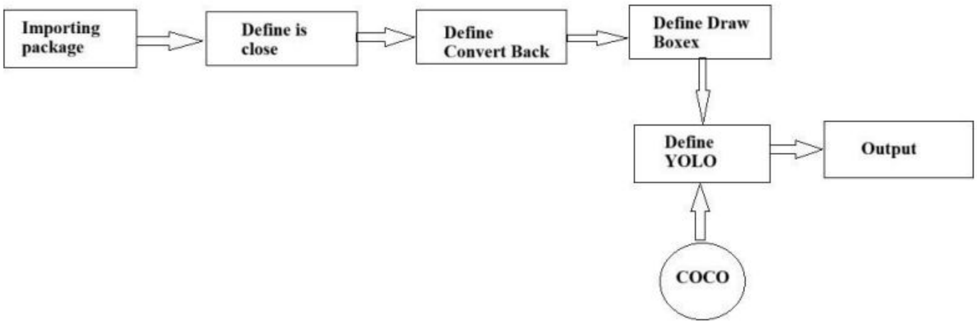
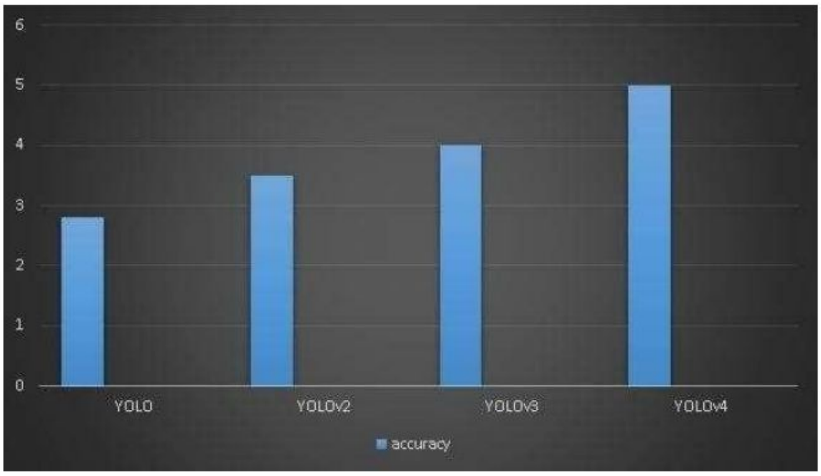


Figure 6: YOLO Darknet Architecture Image by Author

The architecture for the analysis of face masks on objects, the objects over here is the person on which the detection is performed with the help of custom datasets. The custom dataset is trained for 3 different categories (Good, None & Bad) depending upon the annotations provided, it bounds the boxes with respective classes. The difference between object detection and object tracking is the use of a tracker (in Yolo Deep Sort) which helps in keeping a track ofan object by assigning an Id.

ANALYSIS AND EXPERIMENTAL RESULTS OF THE PROPOSED SYSTEM

The analysis of a User Authentication System utilizing M-YOLOv4-C for face authentication



Graph: Accuracy rate of YOLO V4

involves evaluating various aspects of the system's performance, accuracy, security, and user experience. Measure the accuracy of face authentication by assessing the system's ability to correctly identify individuals. Evaluate the detection speed to ensure real-time performance, which is crucial for practical applications. Consider the impact of factors such as lighting conditions, pose variations, and occlusions on accuracy.

Understand the architecture of M- YOLOv4-C, including its deep learning components and how it contributes to accurate face recognition. Analyze the efficiency and computational requirements of the model, especially in resource constrained environments.

Compare the performance of MYOLOv4-C with other face authentication methods, considering factors like accuracy, speed, and robustness. Evaluate how M-YOLOv4-C performs in comparison to traditional methods, such as Haar cascades or earlier versions of YOLO. Assess the system's robustness against potential security threats, including adversarial attacks and attempts at identity spoofing. Evaluate the effectiveness of any additional security measures, such as liveness detection, to ensure the presented face is from a live individual. Examine the efficiency of the database management system in storing and retrieving facial embeddings. Analyze the scalability of the system as the size of the user database grows

CONCLUSION

The substantial advancement of deep learning technology is covered in the paper, with special attention to image recognition with the M-YOLOv4-C model—a modification of the YOLO (You Only Look Once) architecture. Applications of deep learning include voice and image recognition, and it is now a key component of developing markets like autonomous vehicles and crime prevention monitoring systems.

A Closed-Circuit Television (CCTV) system employs the M-YOLOv4-C model to detect a visitor's face and identify 81 feature points in the face. Based on these features, a set of vector values is generated. A database contains the face images of family members who have pre- registered. The paper discusses the rapid advancement of deep learning technology, particularly in image recognition using the M-YOLOv4-C model, a variant of the YOLO (You Only Look Once) architecture. Deep learning has found applications in voice and image recognition, and it is now playing an important role in emerging industries such as autonomous driving and crime prevention monitoring systems.

The M-YOLOv4-C model is used in a Closed-Circuit Television (CCTV) system to detect a visitor's face and recognize 81 feature points in the face to generate a set of vector values based on The suggested model's evaluation metrics using M-YOLOv4-C are given. In particular, the inference time for Tiny-YOLOv3 is 6.5 FPS with an accuracy of 86.3%, and for YOLOv3, it is reported as 2.4 frames per second (FPS) with an accuracy of 90.3%.these features. Face images of pre-registered family members are saved in a database. The system is programmed to open the front door when a new visitor is identified as a family member. Future research, according to the paper, ought to concentrate on broadening the system's uses, like creating access control systems for stores or eateries. This would entail keeping track of visitors, storing visit records, automatically registering frequent visitors, and limiting access based on visitor recognition. Furthermore, there is a request for the creation of a face recognition-based access authentication system that uses the M-YOLOv4-C model's capabilities as a low-false detection rate substitute for passwords or fingerprints.

REFERENCES:

[1]. Y. Indulkar, "Alleviation of COVID by means of Social Distancing & Face Mask Detection Using YOLO V4," 2021 International Conference on Communication information and Computing Technology (ICCICT), Mumbai, India, 2021, pp. 1-8, doi: 10.1109/ICCICT50803.2021.9510168.

[2]. Y. Indulkar, " Visitor Authentication Based & Face Mask Detection Using YOLO V4," 2020 International Conference and Computing Technology (ICCICT), Mumbai, India, 2021, pp. 1-8, doi: 10.1109/ICCICT50803.2021.9510168.

[3]. Howard A, Sandler M, Chen B, Wang W, et al. Searching for MobileNetV3. In: 2019 IEEE/CVF International Conference on Computer Vision (ICCV). Seoul, Korea(South); 2019.p. 1314- 24.

[4]. H. -J. Mun and M. -H. Lee, "Design for Visitor Authentication Based on Face Recognition Technology Using CCTV," in IEEE Access, vol. 10, pp. 124604-124618, 2022, doi: 10.1109/ACCESS.2022.3223374.

[5]. T. A. Kiran, N. D. K. Reddy, A. I. Ninan, P. Krishnan, D. J. Aravindhar and A. Geetha, "PCA based Facial Recognition for Attendance System," 2020 International Conference on Smart Electronics and Communication (ICOSEC), Trichy, India, 2020, pp. 248-252, doi: 10.1109/ICOSEC49089.2020.9215326.

[6]. J. Zheng, J. Zheng, S. Zhang, H. Yu, L. Kong and D. Zhigang, "Segmentation Method for Whole Vehicle Wood Detection Based on Improved YOLACT Instance Segmentation Model," in IEEE Access, vol. 11, pp. 81434-81448, 2023, doi: 10.1109/ACCESS.2023.3300900.

[7]. A. Boragule, K. C. Yow and M. Jeon, "On-device Face Authentication System for ATMs and Privacy Preservation," 2023 IEEE International Conference on Consumer Electronics (ICCE), Las Vegas, NV, USA, 2023, pp. 1-4, doi: 10.1109/ICCE56470.2023.10043387.

[8]. M. Luo, J. Cao, X. Ma, X. Zhang and R. He, "FA-GAN: Face Augmentation GAN for Deformation-Invariant Face Recognition," in IEEE Transactions on Information Forensics andSecurity, vol. 16, pp. 2341-2355, 2021, doi: 10.1109/TIFS.2021.3053460.

[9]. Alzu‘bi, A.; Albalas, F.; AL-Hadhrami, T.; Younis, L.B.; Bashayreh, A. Masked Face Recognition Using Deep Learning: A Review. Electronics 2021, 10, 2666.

[10]. R. He, X. Wu, Z. Sun, and T. Tan, ―Learning invariant deep representation for NIR-VISface recognition,‖ in Proc. 31st AAAI Conf. Artif. Intell., 2017,pp. 2020-2021.

[11] R. He, X. Wu, Z. Sun, and T. Tan, ―Wasserstein CNN: Learning invariant features for NIR-VIS face recognition,‖ IEEE Trans. Pattern Anal. Mach. Intell., vol. 41, no. 7, pp. 1761–1773, Jul. 2019.

[12] X. Di, B. S. Riggan, S. Hu, N. Short, and V. Patel, ―Polarimetric thermal to visible face verification via self-attention guided synthesis,‖ in Proc. Int. Conf. Biometrics, 2019, pp. 1–8.

[13]. K. Yu, G. Tang, W. Chen, S. Hu, Y. Li and H. Gong, "MobileNet-YOLO v5s: An Improved Lightweight Method for Real-Time Detection of Sugarcane Stem Nodes in Complex Natural Environments," in IEEE Access, vol. 11, pp. 104070-104083, 2023, doi: 10.1109/ACCESS.2023.3317951.

[14]. L. L. Chambino, J. S. Silva, and A. Bernardino, __Multispectral facial recognition: A review,'' IEEE Access, vol. 8, pp. 207871– 207883, 2020, doi: 10.1109/ACCESS.2020.3037451.

[15] K. Kim, B. Lee, and J. W. Kim, __Feasibility of deep learning algorithms for binary classification problems,'' J. Intell. Inf. Syst., vol. 23, no. 1,pp. 95–108, Mar. 2017, doi: 10.13088/jiis.2017.23.1.095.

[16] R. Girshick, J. Donahue, T. Darrell, and J. Malik, __Rich feature hierarchiesfor accurate object detection and semantic segmentation,'' in Proc. IEEEConf. Comput. Vis. Pattern Recognit., Jun. 2014, pp. 580–587.

[17] A. Kumari Sirivarshitha, K. Sravani, K. S. Priya and V. Bhavani, "An approach for Face Detection and Face Recognition using OpenCV and Face Recognition Libraries in Python," 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS)

[18] S. Ren, K. He, R. Girshick, and J. Sun, __Faster R-CNN: Towards real time object detection with region proposal networks,'' IEEE Trans. PatternAnal. Mach. Intell., vol. 39, no. 6, pp. 1137–1149, Jun. 2016.

[19]. P. Mary Jenifer, P. Mahasri, A. Omsai, B. I. Humaira and R. Dhnaalakshmi, "Multiple Face Detection and Attendance System Using OpenCV," 2021 International Conference on Simulation, Automation & Smart Manufacturing (SASM), Mathura, India, 2021, pp. 1-5, doi:10.1109/SASM51857.2021.9841223.

[20] W. Fang, L. Wang, and P. Ren, __TinierYOLO: A real-time object detection method for constrained environments,'' IEEE Access, vol. 8,pp. 1935–1944, 2020, doi: 10.1109 /ACCESS.2019.2961959.

[21] K. M. Lee, H. Song, J. W. Kim, and C. H. Lin, __Balanced performancefor efficient smallobject detection YOLOv3-tiny,'' in Proc. Korean Soc.Broadcast Eng. Conf. Anseong, South Korea: The Korean Institute ofBroadcast and Media Engineers, Nov. 2018, pp. 117–118

[22]. Pedoeem J, Huang R, Chen C. YOLO-LITE: A real-time object fetection algorithm optimized for non-GPU computers. In: 2018 IEEE International Conference on Big Data (Big Data). Seattle, WA, USA; 2018. p. 2503-10.

[23]. Bochkovskiy A, Wang CY, Liao HYM. YOLOv4: Optimal speed and accuracy of objectdetection. arXiv preprint; 2020: arXiv:2004.10934.

[24] Howard A, Sandler M, Chen B, Wang W, et al. Searching for MobileNetV3. In: 2019 IEEE/CVF International Conference onComputer Vision (ICCV). Seoul, Korea(South); 2019.p. 1314-24

[25]. Wang K, Chen C, He Y. Research on pig face recognition model based on keras convolutional neural network. In: Proceeding of the 2nd International Conference on Environmental Prevention and Pollution Control Technologies (EPPCT2020). Sanya, Hainan, China; 2020. p. 411-20.

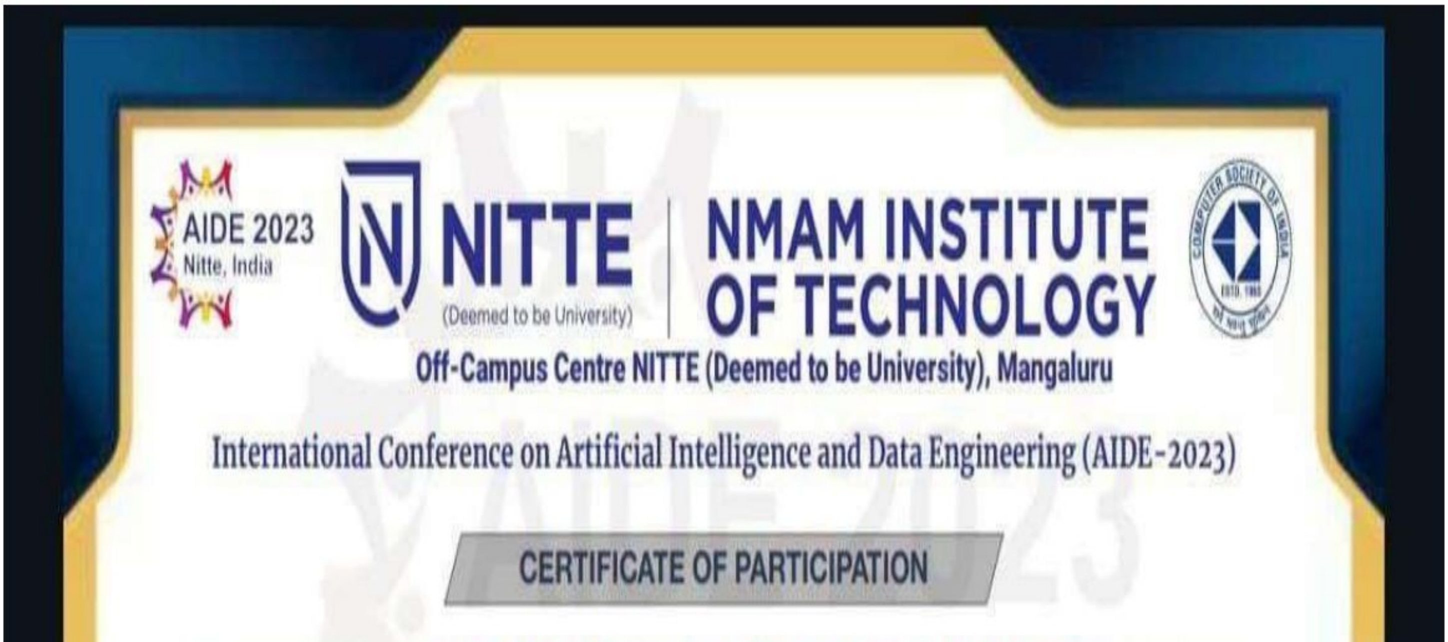
[26]. M. Alsawwaf, Z. Chaczko, M. Kulbacki, and N. Sarathy, __In your face:Person identification through ratios and distances between facial features,''Vietnam J. Comput. Sci., vol. 9, no. 2, pp. 187–202, May 2022, doi: 10.1142/S2196888822500105

[27] S. Han, __Age estimation from face images based on deep learning,'' inProc. Int. Conf. Comput. Data Sci. (CDS), Stanford, CA, USA, Aug. 2020,pp. 288–292, doi: 10.1109/CDS49703.2020.00063.

[28] Q. Guo, Z. Wang, C. Wang, and D. Cui, __Multi-face detection algo rithm suitable for videosurveillance,'' in Proc. Int. Conf. Comput. Vis.,Image Deep Learn. (CVIDL), Chongqing, China, Jul. 2020, pp. 27–33, doi:10.1109/CVIDL51233.2020.00013.

[29] M. Waseem, S. A. Khowaja, R. K. Ayyasamy, and F. Bashir, __Facerecognition for smart door lock system using hierarchical network,'' inProc. Int. Conf. Comput. Intell. (ICCI), Seri Iskandar, Malaysia, Oct. 2020,pp. 51–56, doi: 10.1109/ICCI51257.2020.9247836.

[30] H.-J. Mun and K.-H. Han, __Design for access control systembased on voice recognition for infectious disease prevention,''J. Korea Converg. Soc., vol. 11, no. 7, pp. 19–24, Jul. 2020, doi:10.15207/JKCS.2020.11.7.019.



AIDE 2023
Nitte, India

NITTE
(Deemed to be University)

NMAM INSTITUTE
OF TECHNOLOGY

Off-Campus Centre NITTE (Deemed to be University), Mangaluru

International Conference on Artificial Intelligence and Data Engineering (AIDE-2023)

CERTIFICATE OF PARTICIPATION

This is to certify that **Shashank S Biradar,Pradeep V, Likhita KM, Ravindra , Suraj Ankolekar** has authored a research paper titled **Visitor Face Authentication Using Deep Learning** in **International Conference on Artificial Intelligence and Data Engineering (AIDE-2023)** organized by NMAM Institute of Technology, Nitte in association with CSI Bangalore Chapter of NMAM Institute of Technology, Nitte, Karkala held during 19th to 20th December, 2023.

Jyothi Shetty

Ashish Singh

Dr. Jyothi Shetty   Dr. Sharada U Shenoy
Organizing Chairs

Dr. Udaya Kumar K Shenoy   Dr. Ashish Singh
Conference Secretaries

Niranjan N Chiplunkar
Principal, NMAMIT, NITTE

APPENDIX-B

PROJECT ASSOCIATES INFORMATION

	Ms. Likhita K M pursuing Bachelor of Engineering in Information Science and Engineering from Visvesvaraya Technological University. She is a student of Alva's Institute of Engineering and Technology, Mijar, Moodbidri. Email-ID: likhitamgowda@gmail.com Contact no: 9380454063
	Mr. Ravindra Reddy pursuing Bachelor of Engineering in Information Science and Engineering from Visvesvaraya Technological University. He is a student of Alva's Institute of Engineering and Technology, Mijar, Moodbidri. Email-ID: ravindrareddykothakapu@gmail.com Contact no: 8105190830
	Mr. Shashank Biradar pursuing Bachelor of Engineering in Information Science and Engineering from Visvesvaraya Technological University. He is a student of Alva's Institute of Engineering and Technology, Mijar, Moodbidri. Email-ID: shashanksatishkumar10@gmail.com Contact no: 8050761361
	Mr. Suraj Ankolekar pursuing Bachelor of Engineering in Information Science and Engineering from Visvesvaraya Technological University. He is a student of Alva's Institute of Engineering and Technology, Mijar, Moodbidri. Email-ID: surajankolekar@gmail.com Contact no: 9480507243
	Dr. Pradeep V Associate Professor, Department Information Science and Engineering from Visvesvaraya Technological University. Alva's Institute of Engineering and Technology, Mijar, Moodbidri. Email-ID:writetopv@gmail.com Contact no: 9487626085