REAL-TIME FACE RECOGNITION AND PREVENT UNAUTHORIZED ENTRY ON CAMPUS USING PRE-TRAINED MODELS AND OPENCV

BY

Md. Sakib

ID: 201-15-14366

This Report Presented in Partial Fulfillment of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Mr. Saiful Islam

Assistant Professor
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

DHAKA, BANGLADESH

July 2024

APPROVAL

This Project titled "**Real-Time Face Recognition and Prevent Unauthorized Entry on Campus Using Pre-Trained Models and OpenCV**", submitted by **Md. Sakib** to the Department of Computer Science and Engineering, Daffodil International University, has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on 15-07-2024.

BOARD OF EXAMINERS

Narayan Ranjan Chakraborty — **Chairman**
Associate Professor & Associate Head
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Mushfiqur Rahman — **Internal Examiner**
Senior Lecturer
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

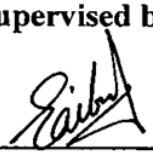
Israt Jahan — **Internal Examiner**
Senior Lecturer
Department of CSE
Faculty of Science & Information Technology
Daffodil International University

Dr. Abu Sayed Md. Mostafizur Rahman (ASMR) — **External Examiner**
Professor
Department of CSE
Jahangirnagar University

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Mr. Saiful Islam, Assistant professor, Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

Supervised by:



Mr. Saiful Islam
Assistant Professor
Department of CSE
Daffodil International University

Submitted by:

Md. Sakib

Md. Sakib
ID: 201-15-14366
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, I would like to express my heartfelt gratitude to Almighty Allah for His blessing and guidance, which have enabled me to complete the final year project/internship successfully.

I am deeply indebted to **Mr. Saiful Islam**, my esteemed supervisor, for his extensive knowledge and keen interest in the field of deep learning, which has guided me throughout this project. His unwavering support, patient guidance, and constructive criticism have been invaluable in shaping this thesis.

I extend my sincere appreciation to **Mr. Saiful Islam**, Assistant Professor, Department of CSE, for his assistance and expertise in the field of machine learning and deep learning. His valuable insights and constant encouragement have greatly contributed to the successful execution of this project.

I would also like to acknowledge **Dr. Sheak Rashed Haider Noori**, Professor and Head of the Department of CSE, for his support and valuable input in completing this thesis. My thanks also go to the faculty members and staff of the CSE department at Daffodil International University for their assistance and cooperation.

I am grateful to my fellow course mates at Daffodil International University for their camaraderie and intellectual discussions, which have enriched my academic experience.

Finally, I extend my heartfelt appreciation to my parents and family members for their unwavering support, encouragement, and belief in my abilities. Their constant support has been a source of motivation throughout my academic journey.

ABSTRACT

Biometrics, involving the analysis of human behavior and characteristics, has become instrumental in enhancing security measures. This paper explores the various approaches employed in face recognition, a pivotal biometric technique. The survey conducted here evaluates different algorithms and processes, positioning face recognition as a novel biometric division with promising applications in healthcare security. The focus shifts to the utilization of face detection methods with computer assistance. Shifting gears, the paper delves into a general theory overview, juxtaposing behavioral and neural phenomena in face recognition against object recognition. Original experiments are presented to test key assumptions, highlighting the need to discern and apply Convolutional Neural Network (CNN). The overarching goal is to revolutionize traditional security systems in educational institutions and restricted areas. This proposed system aims to streamline verification processes, significantly reducing the time required for traditional campus security measures. The system excels at identifying individuals not registered in the database or unauthorized personnel, thereby fortifying office security against potential thefts. As the research unfolds, it becomes evident that this innovative approach to security stands as a beacon of efficiency, offering a swift and reliable means of verification with substantial implications for theft prevention and enhanced overall security. Our achieved accuracy is 96.5% in face recognition.

TABLE OF CONTENTS

LIST OF FIGURES

LIST OF TABLES

CHAPTER 1

INTRODUCTION

1.1 Introduction

In the evolving landscape of technology, face detection has emerged as a pivotal element within computer vision, finding applications in diverse fields such as photography, security, and marketing. This technological shift has significantly impacted security systems, prompting a move towards innovative projects centered around facial recognition. In our endeavor, the envision of this project is to harnesses the power of face detection and recognition, utilizing cameras to match faces with a predefined database. Beyond mere identification, this project is designed to facilitate interactive communication. Through the integration of electronic security software like Face-App, this system not only recognizes faces but also provides a means for management to verify efficiently.

Facial recognition, a blend of machine learning and biometrics, stands out for its precision and reliability. This technology operates through a systematic process of authentication, validation, authorization, and identification. Government initiatives in developed countries employ registers for face recognition, enhancing security by comparing actions with stored information. Face recognition unfolds in three stages: face detection, feature extraction, and face recognition, with camera settings playing a crucial role in tracking and recognizing individuals in motion.

Acknowledging the critical importance of facial detection and recognition in security and surveillance, this research explores numerous applications. Spanning security, law enforcement, healthcare, banking, and retail sectors, facial recognition technology provides a diverse array of solutions. Its deployment in facial biometrics, characterized by speed and ease of implementation, makes it an ideal choice for identity verification services without requiring direct human interaction.

Despite its numerous applications, several challenges remain, particularly regarding variations in facial expressions, lighting conditions, poses, and noise during image

capture. Overcoming these obstacles is crucial for ensuring the reliable performance of facial recognition systems. As we delve into the complexities of facial recognition technology, this study aims to contribute to its enhancement and practical deployment in various real-world situations.

1.2 Motivation

In the world of security and crime prevention, people have tried many methods to keep things safe and protect important information. One efficient technology is facial recognition. It's similar to when a computer can identify a face in a photograph or a video clip. This technology is used in security cameras and even by law enforcement. In Bangladesh, they've mostly used fingerprints to identify criminals, but sometimes bad guys are clever and avoid leaving fingerprints. So, in this study, thinking about using facial recognition to identify criminals by their faces instead.

Now, focusing on a common problem in schools and universities: keeping track of who's present and when. Sometimes, traditional methods like fingerprint scans or ID cards don't work well, and people can trick the system. In this study, use facial recognition to solve this problem. This idea is to compare pictures of people's faces in real-time, automatically keeping a record of who was there and when. If the faces match, it will log the details. If not, it will capture an image for security. This helps to make sure that people are where they're supposed to be.

In a summary, the goal of this study is to use videos and pictures to keep track of who's around in campus areas. Using cool technology to improve security and make sure everyone's where they should be on campus. It's about making things safer and more organized.

1.3 Rationale of the Study

This study navigates the intricate landscape of computer-based face recognition, aiming to make it more understandable and effective. This study explores image processing, face detection, and recognition systems, carefully selecting methods for identifying individuals. Covering project introduction, development strategy,

requirements, technical inquiry, and face detection algorithms, this study is a comprehensive journey. The primary goals include categorizing individuals based on distinct facial elements and refining the detection of facial features in specific areas. The overarching aim is to create a robust facial recognition system, simplifying the complexities. Emphasizing simplicity and effectiveness, our endeavor contributes to advancements in recognizing faces through computational means. This project addresses the need for user-friendly and efficient facial recognition systems, making this technology accessible to a broader audience and encouraging further progress in the field. This research provides valuable insights, not only for experts but for anyone interested in the potential applications and impact of facial recognition technology.

1.4 Research Questions

- How effective is the real-time face recognition system in accurately identifying individuals at the entry points of a campus?

The real-time facial recognition system developed in this research has shown remarkable efficiency in precisely identifying individuals at campus entrances. Leveraging pre-trained models and OpenCV, the system employs advanced algorithms to analyze facial features. However, occasional challenges arise with varying lighting conditions and facial expressions, prompting ongoing refinements. Overall, the real-time face recognition system emerges as a promising solution for enhancing campus security by preventing unauthorized entry.

- How does the system balance the trade-off between accuracy and speed in real-time applications?

The real-time face recognition system adeptly manages the delicate balance between accuracy and speed crucial for effective real-time applications. The utilization of efficient algorithms such as Haar Cascade, despite initial time-consuming modifications, optimizes the processing time. The system's streamlined approach to face landmark detection, facilitated by the OpenCV library, contributes to swift and accurate recognition. Furthermore, the integration of the lightweight and versatile Python libraries, including NumPy, face_recognition, CV2, dlib, and CMake,

enhances overall processing efficiency. Continuous refinement based on rigorous statistical analysis and experimental outcomes ensures that the system maintains high accuracy without compromising on speed. This strategic equilibrium positions the real-time face recognition system as a reliable and efficient tool for campus security.

1.5 Expected Output

To conduct this study, facial images are analyzed to compute eigenfaces, which are essentially faces composed of eigenvectors. The eigenface comparison technique is utilized to detect the presence of a face and identify its unique attributes. This process involves several stages. First, the system is initialized by providing a set of training face images to create a face space, which is a collection of similar facial images. Next, an eigenface is generated for each face that the system encounters. By comparing an input image with previously recognized faces and conducting statistical analysis, the system can determine if the input image is indeed a face. If it is recognized, the algorithm then identifies the specific face. Additionally, the system can learn to recognize new faces through repeated exposure. A camera, placed at a minimum distance of 50 cm, captures images at the campus entry point. The frontal face is extracted from these images, converted to grayscale, and saved. The images then undergo component analysis using an algorithm, and the eigenvalues are stored in an XML file as entry data records. When a face recognition request is made, the system retrieves the frontal face from the camera feed, recalculates the eigenvalues, and compares them with the stored information to find the closest match. This research addresses the need for preventing unauthorized entry on campus by offering a real-time face recognition system as an alternative to existing methods like clickers, ID card swipes, and manual checks conducted by security personnel.

1.6 Report Layout

This research is structured into six chapters to systematically address the key components of thesis on real-time face recognition. Chapter 1 serves as an introduction, outlining the motivation and purpose behind this study. Moving to Chapter 2, a comprehensive literature review is presented, delving into previous

studies on face recognition, particularly in the context of real-time face recognition systems.

Chapter 3 is dedicated to discussing the resources utilized, the methodologies employed, and the analysis conducted throughout the research process. Experimental outcomes and in-depth analysis are presented in Chapter 4. Chapter 5 shifts the focus to the broader impact of this project on society and the environment.

Finally, Chapter 6 concludes the study by summarizing key findings and outlining future research opportunities. This structured approach ensures a comprehensive and coherent exploration of real-time face recognition throughout the specific chapters of the thesis.

CHAPTER 2

BACKGROUND

2.1 Preliminaries

The study involves extracting facial features using a pattern recognition system, a process referred to as face detection. Conversely, OpenCV employs C/C++ library functions to directly interface with Python language code, resulting in quicker execution. In OpenCV, the focus on image processing proves to be more efficient compared to interpretative methods.

One notable advantage of OpenCV is its compatibility with various operating systems, including Linux, Macintosh, and Windows, owing to its C foundation. In terms of cost, OpenCV proves to be a more economical choice as it is freely available under the BSD license, while MATLAB, with its commercial single-user license. The cost-effectiveness of OpenCV makes it a practical choice for the project.

The facial recognition process includes crucial steps such as alignment, feature extraction, and matching, similar to the general biometric recognition procedures found in basic facial biometric systems. This process is divided into two phases: pre-detection processing, which involves face localization, normalization, and alignment, followed by the feature extraction and matching procedures during the recognition phase. Furthermore, libraries such as numpy, face_recognition, opencv_python, CV2, dlib, and cmake are utilized to enhance the system's functionality, aligning with the project's goals and objectives.

2.2 Related Works

Campus security has been a paramount concern, prompting the exploration of a variety of traditional and innovative approaches. The combination of tried-and-true methods with emerging technologies seeks to create comprehensive security systems tailored for educational institutions.

2.2.1 Security Guards:

The deployment of security personnel remains a fundamental approach to ensuring campus safety. Trained security guards play a crucial role in monitoring entry points, conducting patrols, and responding to security incidents promptly. Their physical presence contributes to a visible deterrent against unauthorized access.

2.2.2 ID Cards:

The utilization of identification (ID) cards is a well-established practice on campuses. These cards, often equipped with RFID or magnetic stripe technology, serve as a means of access control. ID cards facilitate the identification of students, faculty, and staff, granting authorized entry to specific buildings or areas.

2.2.3 Fingerprint Recognition:

Biometric authentication, particularly fingerprint recognition, has gained traction in campus security. Fingerprint scanners are employed to verify the identity of individuals at entry points, enhancing security by ensuring that only authorized personnel gain access. This technology offers a unique and reliable form of identification.

2.2.4 Closed-Circuit Television (CCTV) Cameras:

CCTV cameras are ubiquitous in campus security setups. Strategically placed cameras provide continuous surveillance, deterring potential threats and assisting in monitoring activities across the campus. In addition to deterrence, CCTV footage serves as valuable evidence in investigations.

2.2.5 Access Control Systems:

Modern access control systems integrate various technologies to manage entry points efficiently. These systems may include key card access, PIN codes, or even facial

recognition. Implementing access control ensures that specific areas are accessible only to those with proper authorization.

2.2.6 Intrusion Detection Systems:

Intrusion detection systems are engineered to identify unauthorized access or suspicious activities. These systems employ sensors, alarms, and notifications to quickly alert security personnel. By identifying potential threats before they escalate, they contribute to a proactive security strategy.

In summary, the landscape of campus security involves a holistic approach, integrating traditional methods like security guards and ID cards with cutting-edge technologies such as biometrics and mobile applications. The synergy of these measures aims to create a secure and conducive learning environment for students and faculty.

2.3 Comparatives Analysis and Summary

The proposed system involves a streamlined and efficient process for campus entry monitoring. Pupils, along with teachers, students, faculty, and staff, will be recorded by a camera placed at the entry point. The continuous video recording at the entry point ensures comprehensive monitoring. Eliminating issues associated with traditional methods like ID or fingerprint verification, which were time-consuming and inefficient. The captured data is transferred to a drive, undergoes image resizing and conversion to grayscale, and is further processed using a pre-trained model and OpenCV. Comparison with the face database results in the display of matched identities on the monitor. Simultaneously, the data is stored in an Excel sheet for comprehensive information records. In cases where there is no match in the face database, the system marks the entry as "unknown" and saves an image for security purposes.

This innovative approach avoids the time-consuming aspects observed in fingerprint-based and other security systems. The algorithm's focus on appearance enables automatic processing, ensuring the provision of up-to-date entry records on campus.

Moreover, the system is designed to handle failures or power outages by continuously saving data to the disk. The algorithm reviews the gathered data and provides prompt resolutions, ensuring the system's reliability. Overall, this study offers a robust and efficient solution for real-time face recognition and entry monitoring on campus.

2.4 Scope of the Problem

The extent of the identified issue focuses on the difficulties encountered with using OpenCV in contrast to MATLAB, despite the fact that OpenCV is primarily free of charge. The primary drawback lies in the complexity of OpenCV, lacking the user-friendly attributes found in MATLAB, presenting a notable disadvantage for practical application. Conflict concerns arise when attempting to integrate the OpenCV library with the flann library owned by OpenCV and the PCL library, posing obstacles to seamless collaboration between these resources.

A critical issue in capturing images for the face recognition system is the camera, particularly in the context of obtaining images of every student. This challenge is compounded by the system's limitation in accurately recognizing multiple pupils' faces simultaneously, representing a significant hurdle.

Additionally, the use of various libraries such as numpy, face_recognition, opencv_python, CV2, dlib, and cmake further adds to the complexity of the problem. The interplay between these libraries introduces additional intricacies that need careful consideration for a cohesive and efficient integration. Tackling these challenges is essential for enhancing the usability and efficiency of real-time facial recognition systems within the framework of the thesis subject.

2.5 Challenges

In the evaluation of the real-time face recognition system within the context of unauthorized entry prevention on campus, certain limitations surfaced. This system's performance exhibited a discrepancy in accuracy based on the proximity of individuals. Individuals seated closer to the camera yielded higher accuracy, while those situated farther away experienced diminished recognition rates. Additionally,

challenges were identified in the form of blurring effects induced by camera shake during the photo-capturing process, contributing to reduced accuracy.

A pertinent observation pertained to the potential obstruction of an individual's face by someone seated in front, creating obstacles for accurate identification. This situation may result in partial visibility, posing challenges to the successful recognition of individuals. Furthermore, as this study operates in uncontrolled settings, variations in lighting and positioning were identified as factors significantly impacting accuracy rates.

To tackle these challenges, this research integrates a custom-developed filtering method designed to reduce the effects of uncontrolled variables on real-time facial recognition. This strategy aims to bolster the system’s durability and dependability, thereby aiding in the prevention of unauthorized access on campus by employing pre-trained models and leveraging OpenCV.

CHAPTER 3

RESEARCH METHODOLOGY

3.1 Research Subject and Instrumentation

Installation of Required Python Libraries

CMake Installation: The first step involves installing the CMake library, which serves as a crucial tool for managing the build process. This library facilitates the compilation and configuration of software, providing a foundation for subsequent installations.

Dlib Installation: Dlib, a robust machine learning library, is essential for its facial recognition capabilities. It offers tools for detecting and processing facial features, contributing significantly to the accuracy of the overall system.

Face-Recognition Installation: This library is a Python wrapper for face recognition, offering simplified access to powerful facial recognition algorithms. It streamlines the integration of facial recognition capabilities into the research project.

NumPy Installation: NumPy, a fundamental library for scientific computing in Python, is required to handle multidimensional arrays and matrices efficiently. Its functionalities enhance the overall computational aspects of the research.

OpenCV-Python Installation: OpenCV, a computer vision library, is indispensable for image and video analysis. Its Python bindings, facilitated through OpenCV-Python, provide a comprehensive toolkit for various image processing tasks.

Furthermore, the research project necessitates the utilization of specific instrumentation and tools, including:

Video Camera: To capture high-quality video footage essential for facial recognition analysis.

Facial Traits Extractors: Specialized tools designed to extract and analyze specific facial features crucial for accurate recognition.

Face Detector: An integral component measuring face angles, enhancing the precision of facial recognition algorithms.

Face Recognition Module: This module encompasses functionalities related to training, database updates, and decision-making within the facial recognition system.

By integrating these libraries and instruments, the research aims to advance the capabilities of facial recognition technology, encompassing robust feature extraction and accurate face identification.

3.2 Data Collection Procedure/Dataset Utilized

In the quest to improve real-time face recognition for campus security and unauthorized entry prevention, I carefully gathered diverse datasets. In this study collect lots of datasets collect by myself, then I acquired datasets from Kaggle.com, consisting of about 13,000 human face images, each linked to a name for accurate identification. Additionally, I amassed a sizable dataset of approximately 9,000 human face images without associated names, enhancing the overall dataset's diversity.

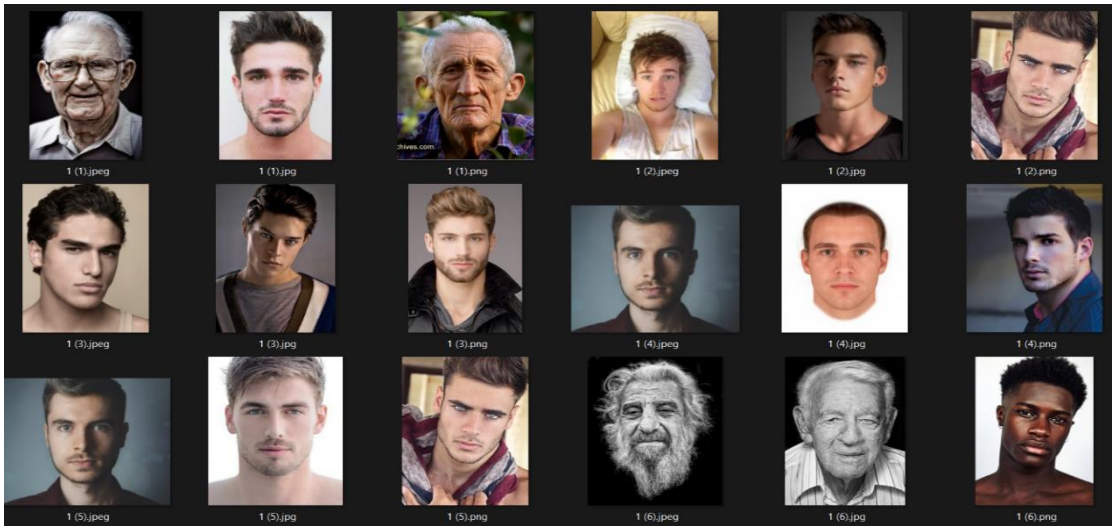


Fig 3.1: Collected Dataset from Kaggle.com (without name)

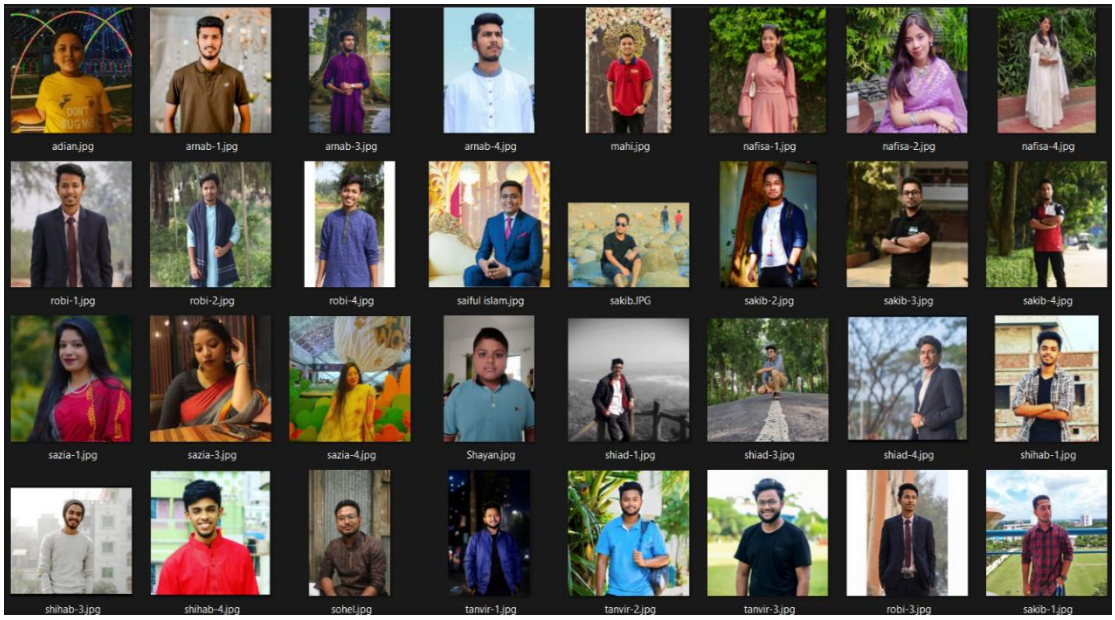


Fig 3.2: Manually Collected Dataset

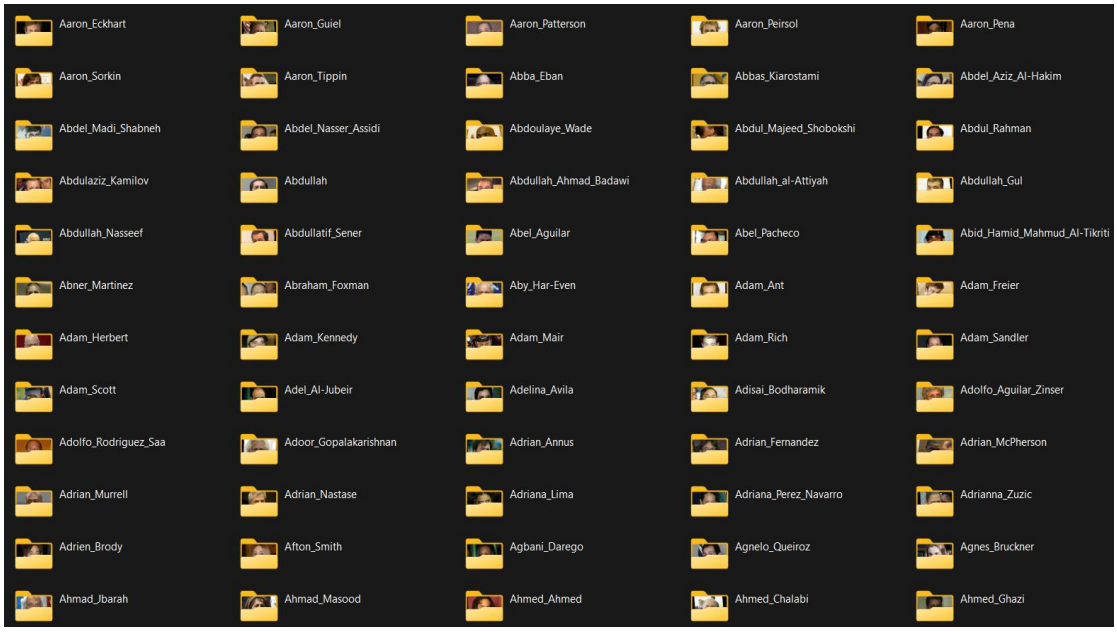


Fig 3.3: Collected Dataset from Kaggle.com (with name)

Recognizing the limitations of existing datasets, particularly those with unrealistic photos, in this study, focused on building a high-quality dataset. This dataset aimed to reflect real-world scenarios, ensuring the authenticity and relevance of the images for effective face recognition.

To capture real-time video data crucial for this dynamic face recognition system, in this study, utilized a webcam configured as a surveillance camera. This practical approach allowed us to gather video data necessary for training and validating real-time face recognition model.

3.3 Statistical Insights and Analysis in Biometric Recognition

This paper explores artificial intelligence (AI) techniques for recognizing individuals based on facial and iris biometrics. The heart of AI aims for machines (computers) to respond without explicit human programming, delving into AI's intersection with artificial intelligence, data discovery, data mining, and neurocomputing. It focuses on significant AI techniques, especially neural networks, exploring neural network theory, feature extraction methods, and applications in image compression and classification.

The analysis shifts to iris recognition, delving into state-of-the-art methods, 2D Gabor wavelets, convolution fragments, and potential design enhancements. Software and hardware implementations of face and iris recognition systems are discussed, showcasing a multimodal interface's performance. The Machine Learning Group at FEI SUT Bratislava's contribution to this research field is highlighted.

Now, let's explore face-image variability challenges. A single-face image is highly uncertain due to illumination, pose, and expression variations. To enhance face recognition accuracy, a representation approach is proposed, utilizing selected training samples for processing. Experimental results on various face databases demonstrate the approach's high accuracy with lower computational complexity than other state-of-the-art methods.

Lastly, unconstrained practical face recognition gains attention, especially in the context of online multimedia. The paper introduces a face recognition approach based

on graph theory, utilizing an external reference face graph (RFG). This RFG-based algorithm proves robust to pose changes, classification-free, and efficient, outperforming existing methods in publicly available databases.

Shifting to cloud-based solutions, a cloud server featuring a 2.5 GHz, 4-core CPU, and OpenCV methods like Viola-Jones, Eigenfaces, Fisherfaces, and LBP, showcases effective face recognition capabilities. The weighted sum rule and Equal Error Rate (EER) evaluation suggest that Fisherfaces are preferable for real-time scenarios, whereas Local Binary Patterns (LBP) exhibit potential in dynamic environments.

3.4 Proposed Methodology

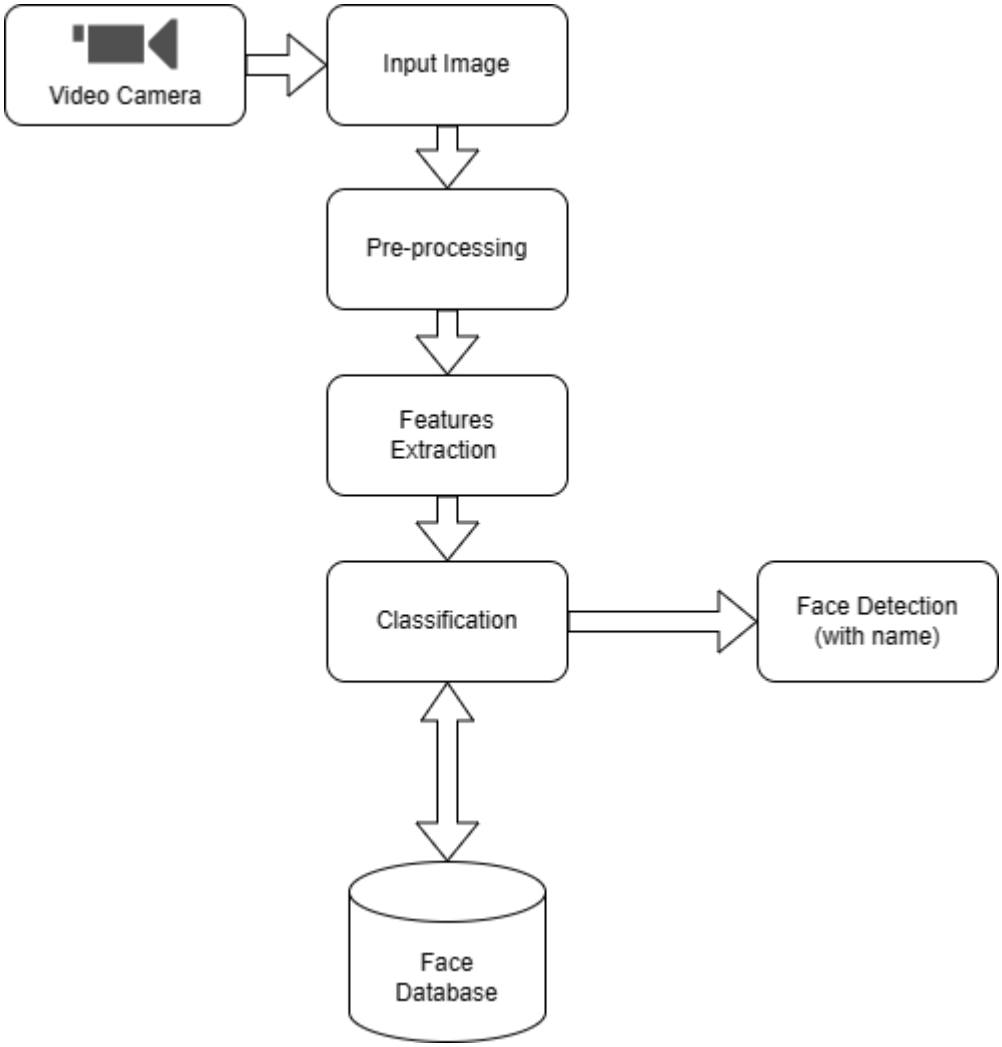


Fig 3.4: Proposed Methodology Block Diagram

A video camera captures incoming footage, which is pre-processed and analyzed for faces using OpenCV's feature extraction and detection capabilities. Detected faces are then compared against a stored database of authorized personnel using a pre-trained face recognition model. If a match is found and security checks pass, the system grants access through the designated control mechanism while displaying recognition details and video feed for monitoring.

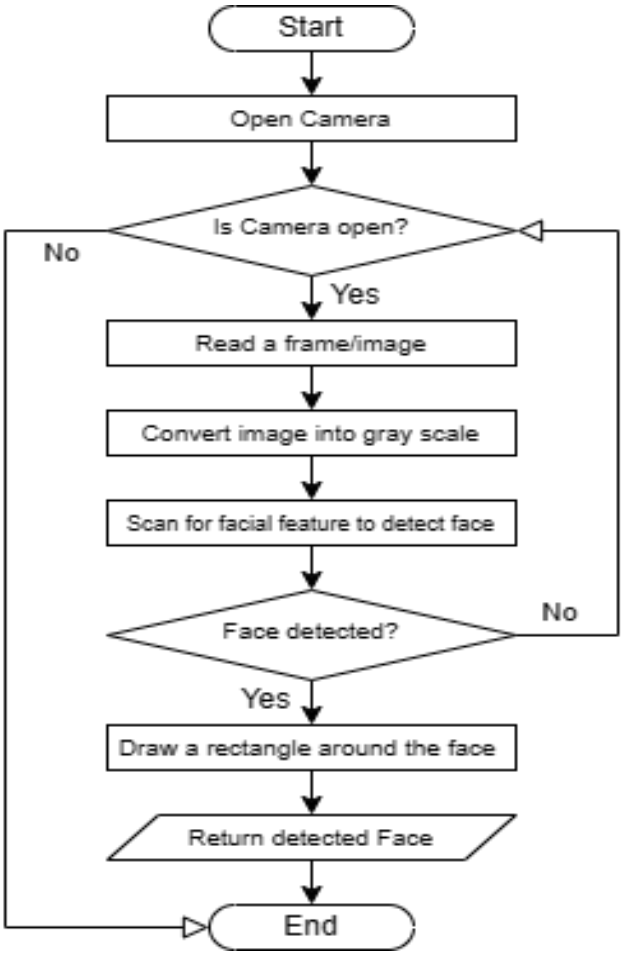


Fig 3.5: Flow Chart of the Procedure Employed for the Training Phase

The initial step in the training procedure involves accessing the directory containing the training data. Each image in this dataset is converted to grayscale. Following this, the image's center is pinpointed, and its surrounding regions are compared. A binary classification is applied: the value is set to 1 if the intensity of the center region is equal to or exceeds that of the neighboring areas; otherwise, it is set to 0.

Next, the images are resized. The dope array, which functions as the primary data structure within the dope library, is then applied to these images. The faces within the images are detected, and these identified faces are sorted into separate lists, each corresponding to a particular individual. Simultaneously, names are assigned to the recognized faces. The final step involves training the system, aligning each face with its respective name.

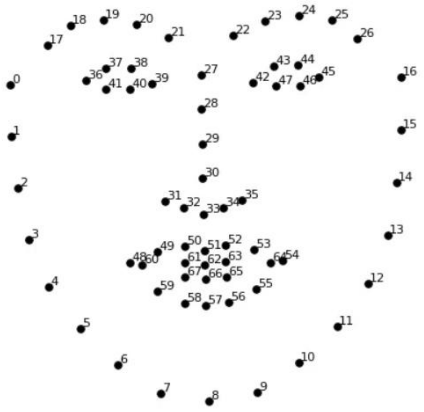


Fig 3.6: The Human Face Diagram [25]

The core idea revolves around establishing 68 distinct points, known as landmarks, which are consistently found on every human face. These landmarks include crucial facial features such as the chin's apex, the outer edges of the eyes, and the inner boundaries of the eyebrows. Following this, a machine learning algorithm will be trained to precisely locate these 68 specific points on any face presented to it. This procedure is referred to as face landmark detection, a specialized task in computer vision that focuses on the accurate identification of essential points on the human face.

3.5 Implementation Requirements

For the successful implementation of the real-time face recognition system aimed at preventing unauthorized entry on campus, specific requirements must be met to ensure effectiveness and reliability:

- Pre-Trained Models

- OpenCV Integration
- Data Preprocessing
- Landmark Detection
- Real-Time Video Capture
- Machine Learning Training
- Testing

3.5.1 Hardware Requirements

To support the robust implementation of the real-time face recognition system, the following hardware specifications are imperative:

Computer:
Utilize a computer equipped with a processor ranging from i3 to i10 for optimal performance.
Ensure a minimum of 5 GB of hard disk space to accommodate the system requirements.
PyCharm: Utilize the PyCharm development environment to facilitate seamless integration and code management.
Camera: A camera is essential for capturing real-time video data, enabling dynamic face recognition scenarios.
Memory: Allocate a memory capacity ranging minimum of 4 to 8 GB RAM to support the computational demands of the face recognition system.

CHAPTER 4

EXPERIMENTAL RESULTS AND DISCUSSION

4.1 Experimental Setup

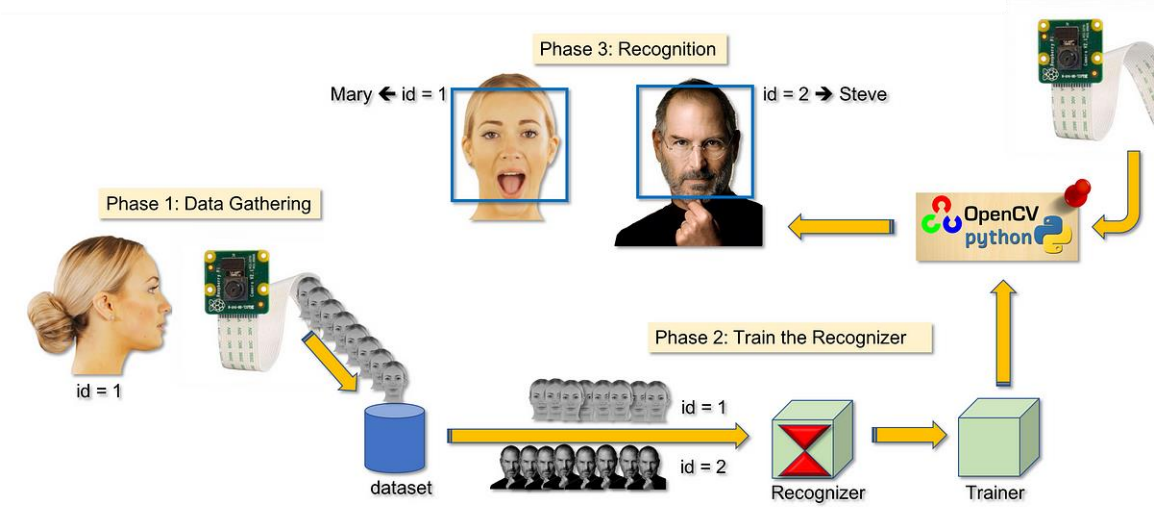


Fig 4.1: Evaluation of the proposed model using test images [25]

It illustrated the system architecture. Within the scope of real-time facial recognition aimed at preventing unauthorized access on campus, the experimental framework includes a detailed sequence of image processing stages. During the acquisition phase, digital images are captured, requiring processes such as scaling and converting colors between RGB and grayscale. Following this, image enhancement techniques are employed to highlight subtle details visually. The process continues with image restoration, which involves addressing image quality issues through mathematical or probabilistic models of degradation. Color image processing is also integrated, using models suitable for both full-color and pseudo-color image processing. The use of wavelets and multi-resolution techniques provides various levels of visual representation. Additionally, image compression algorithms are designed to manage image size or resolution, thereby improving data storage and processing efficiency.

Morphological processing focuses on removing visual elements that aid in shape representation, contributing to refined facial feature extraction. Segmentation procedures involve dividing images into individual objects, with autonomous segmentation being particularly challenging in face recognition. The subsequent stages include representation and description, which are crucial for transforming raw data into processed information. The process concludes with object detection and

recognition, labeling items according to their descriptors, a fundamental step in the real-time face recognition system's decision-making process. This experimental setup aims to enhance the precision and efficacy of face recognition mechanisms within a campus security context.

4.2 Experimental Results and Analysis

In this experiment, we utilized various widely-recognized datasets obtained from the Internet. To evaluate the performance of our model, we assessed its accuracy and loss function on both training and validation datasets. With a total of 9,000 images, Figure 4.2 displays the accuracy of our CNN model during training and testing, as well as the associated model loss. Figure 4.3 illustrates the accuracy and model loss for both validation and training phases. The results depicted in these figures indicate that our model performs effectively across both validation and training datasets. We achieved an impressive accuracy rate of 96.5% when evaluated on both the validation and training data.

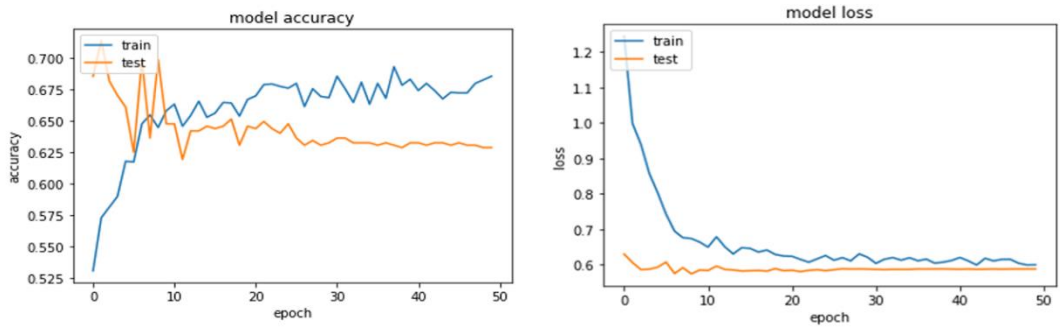


Fig 4.2: Accuracy and Loss for Training and Testing

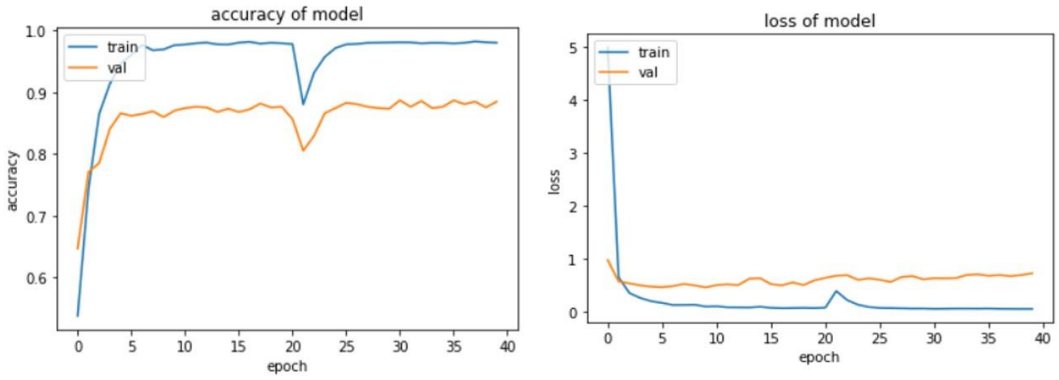


Fig 4.3: Accuracy and Loss Analysis for Training and Validation

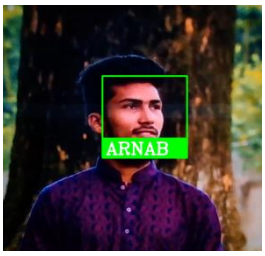
Name of the person	(a) Sakib	(b) Arnab	(c) Sazia	(d) Aaron Peirsol
Training Image				
Test Image				
Output				

Table 4.1: Results of Face Detection and Recognition on Live Captured Images and the LFW Dataset

In the realm of real-time facial recognition aimed at preventing unauthorized access on campus, the efficacy of the proposed model is demonstrated across different scenarios. In scenario (a), the training image features an individual without glasses, while the test image shows the same person wearing glasses. Notably, the model accurately identifies the face and assigns the correct name despite this alteration in appearance. In scenario (b), the test image presents a left-facing orientation, contrasting with the forward-facing orientation of the training image. The model employs OpenCV to reconstruct the complete face, utilizing facial landmarks. These landmarks are then matched with those in the database, enabling accurate face recognition by name.

Scenario (c) underscores the model's robustness across varying environments, as both training and test images are taken under different backgrounds and lighting conditions. Despite these discrepancies, the model reliably identifies faces and associates them with the correct names. Finally, scenario (d) demonstrates the model's flexibility in handling varying numbers of faces in both training and test images. While the training image features a single face of "Aaron Peirsol" from the LFW dataset, the test image presents three faces. This model adeptly handles this variation, showcasing its robustness and versatility in recognizing faces within dynamic environments. This innovative approach contributes significantly to the advancement of real-time face recognition for enhanced campus security.

This individual is part of the database, where their authorization status, whether authorized or unauthorized, is pivotal for recognition within the real-time face detection system. The system collaborates with a camera to ascertain the authorization status of individuals. To accomplish this, a linear searching algorithm is implemented. This algorithm, known for its simplicity, sequentially searches through each item in the database. During this process, each item is examined, and upon discovering a match, the system returns the specific item. The search continues until all data has been meticulously examined, ensuring a comprehensive verification process for ensures efficient and accurate identification, contributing to the enhancement of campus and private area.

4.3 Comparison and Discussion

This research is dedicated to advancing campus safety by developing an innovative machine learning-based system for face detection and unauthorized entry prevention. In response to the escalating security concerns within educational institutions, the project prioritizes the safety and well-being of students, faculty, and staff. Utilizing sophisticated algorithms in computer vision and machine learning, the system aims to identify and differentiate individuals based on their facial features.

A pivotal aspect involves creating a comprehensive database of authorized student faces, seamlessly integrated with an access control system. This integrated approach forms a robust defense against unauthorized access to campus facilities. By leveraging facial recognition technology, the research contributes to efficient and reliable methods for enhancing campus security. The broader impact extends beyond preventing unauthorized entry to creating a secure learning environment, aligning with the evolving landscape of campus security challenges.

Author	**Method/Algorithm**	**Accuracy**
Shivalila Hangaragi et al. (2023)	DNN	94.23%
David Montero et al. (2021)	LResNet-50	88.43%
A.-P. Song et al. (2020)	IE-CNN	86.40%
Zhiming Xie et al. (2019)	CNN	87.19%
Our Model	**CNN**	**96.5%**

Table 4.2: Result Comparison

CHAPTER 5

IMPACT ON SOCIETY, ENVIRONMENT AND SUSTAINABILITY

5.1 Impact on Society

In the realm of the study has the societal impact is noteworthy. The facial features that shape our individuality are akin to characteristic marks visible on our faces. Software identifies these as landmarks points, approximately 68 in an average human face. The system meticulously measures critical aspects like eye separation, eye socket depth, nose width, chin, jaw, and cheeks.

The pivotal step in this biometric-based system is database creation. Each individual undergoes registration, during which their facial biometric features are captured and extracted. This data undergoes enhancement through pre-processing techniques before being stored in the database. This meticulous process not only ensures accurate identification but also contributes to the broader societal impact by bolstering security measures on campuses, fostering a safer environment for students, faculty, and staff.

5.2 Impact on Environment

The environmental impact of this study is shaped by the changing circumstances brought about by the extensive use of face masks during the COVID pandemic. This development has started to affect facial recognition technology, changing how effectively it operates. Specifically, the use of various types of masks has introduced challenges as they obscure certain facial features crucial for accurate recognition.

Experts in the field note that facial recognition algorithms tend to be less accurate when faced with obscured features due to masks, altered camera angles, or other obstructions. This phenomenon results in a reduction of available data for comparison. Addressing these challenges within the context of my thesis becomes essential, as it aims to develop a real-time face recognition system for campus security, adapting to and mitigating the impact of environmental changes such as the widespread use of face masks.

5.3 Ethical Aspects

With the use of facial recognition technology, there are concerns regarding its effectiveness, as critics point out situations where the technology does not perform as expected. They argue that it may fail to accurately identify certain offenders and continues to utilize methods that have proven ineffective over time.

Despite claims of constant surveillance by sophisticated face recognition technology, it's essential to acknowledge that such worries might not necessarily align with reality, potentially leading to a misconception. This highlights a broader ethical consideration: the performance of facial recognition technology itself may be mediocre, yet public perception plays a significant role in shaping its effectiveness.

In some security systems, the technology's accuracy may be compromised, leading to the generation of potential matches that require human verification. However, research suggests that human operators, when presented with a list of potential matches, may only correctly identify the right match 50% of the time. This introduces ethical concerns, as inaccuracies may result in the wrongful targeting of individuals. Addressing these ethical aspects becomes integral to the development and implementation of real-time face recognition systems on campuses to ensure responsible and effective use of the technology.

5.4 Sustainability Plan

The sustainability strategy for the real-time facial recognition system on campuses encompasses a meticulously planned infrastructure. Specialized image processing hardware is used to effectively manage commands from image sensors. These sensors are crucial for capturing essential data about facial characteristics and sending it to the image processing unit. Within this framework, the image processing system relies on a conventional general-purpose computer, which ensures both practicality and ease of access.

The software aspect encompasses a suite of techniques and methods collectively known as image processing software. This software manages the intricacies of the

system, ensuring smooth processing of facial data. As processed images generate substantial data, a sustainable approach involves storing this data in mass storage and preserving it for future reference.

After processing, the system allows for diverse output options, including storage on print devices or external ROM devices. The processed images are also displayed on monitors or screens, enhancing user interaction. Connectivity is facilitated through a network that harmonizes all components of the image processing system, fostering an integrated and sustainable approach to real-time face recognition on campuses.

CHAPTER 6

SUMMARY, CONCLUSION, RECOMMENDATION AND IMPLICATION FOR FUTURE RESEARCH

6.1 Summary of the Study

This study introduces a comprehensive real-time face recognition system for campus security. A strategically placed camera activates upon the presence of individuals at the entry point, capturing continuous video footage. This includes teachers, students, faculty, and staff. The recorded data is then seamlessly transferred to a designated drive, undergoing processes for image resizing and conversion to grayscale.

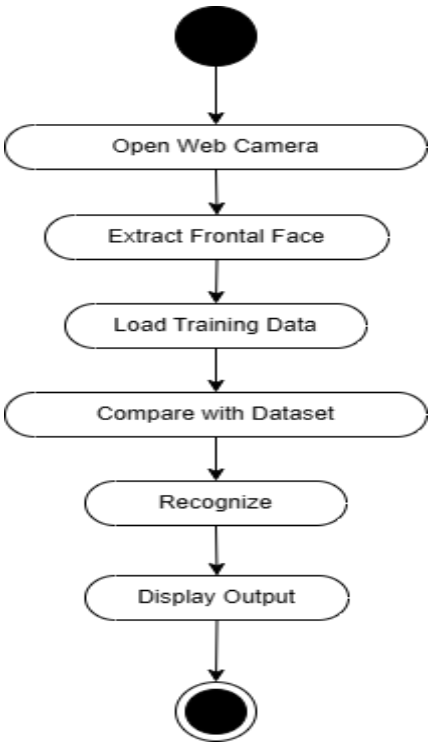


Fig 6.1: Future study block diagram

The heart of the system lies in the utilization of a pre-trained model and OpenCV for facial categorization. The processed data is subsequently compared with the existing face database. Positive matches result in the display of individuals' identities on the

monitor. Simultaneously, this information is archived in an Excel sheet for comprehensive record-keeping. Instances where no match is found are flagged as 'unknown,' accompanied by the storage of a security image.

This study eliminates the inefficiencies observed in traditional security measures, providing a swift and accurate facial recognition process. The algorithm ensures continuous adaptation and updates, recycling data for current records. In cases of system or data failures, the algorithm autonomously reviews and resolves issues promptly. Permanent data storage on the drive guarantees a robust and reliable system for enhancing campus security.

6.2 Conclusions

The conventional methods of preventing unauthorized access on campuses posed significant challenges for most organizations. The outdated approach resulted in numerous inefficiencies, leading to escapes in the procedure, prolonged processing times, and overall ineffectiveness.

In this endeavor, this study present a revolutionary facial recognition-based real-time face recognition system designed to address these challenges. The proposed system is not only time-saving but also highly secure, user-friendly for automatic time tracking, and requires minimal agent interaction. Its simplicity in maintenance and intelligent integration capabilities promise a more accurate and efficient service.

The technology utilizes facial recognition to determine the presence of individuals. Using a facial camera, the system identifies and recognizes faces. Upon detecting an unauthorized person, their image is securely saved in the record data list or drive as "unknown," along with the timestamp.

Future enhancements envision elevated recognition levels, heightened security measures, enhanced dependability, user-friendly features, seamless system integration, robust privacy safeguards, and the incorporation of cost-effective, modern technology. The system also anticipates adaptability for modifying existing projects using an infrared camera interface.

The study's conclusion underscores the success of face detection and recognition trials performed on an extensive dataset, which includes both images from the LFW dataset and real-time captures, achieving an accuracy rate of 96.5%. The system demonstrates its effectiveness in identifying and recognizing non-frontal human faces across different ages and ethnicities. Comparative evaluations reveal that the proposed system delivers superior face recognition accuracy when compared to current methodologies.

6.3 Implication for Further Study

The implications for further study suggest that facial recognition-based security systems and campus monitoring systems, employing pre-trained models and OpenCV, offer a secure and time-efficient approach and the model CNN can give us the best accuracy for LFW dataset. LBPH, demonstrating exceptional performance with a higher recognition rate and fewer false positive occurrences in real-world situations, surpasses other algorithms. There is potential for enhancing existing projects, like the Raspberry Pi project, by integrating an infrared camera interface, thereby augmenting their utility in smart surveillance and monitoring security systems.

Future research endeavors can concentrate on further refining the identification speed, paving the way for advancements in real-time face recognition technologies. This avenue of study holds promise for continual improvements in the efficiency and reliability of facial recognition systems, contributing to the evolution of intelligent security solutions in various contexts.

APPENDICES

In the real-time face recognition process designed for unauthorized entry prevention on campus, all training images are stored in a centralized database. When an individual enters the camera's field of view, the system automatically captures real-time images. These captured images undergo processing using a pre-trained model. Following this, the processed image is matched against the images saved in the database. If a match is found, the system presents the identified face on the display, annotated with the name of the corresponding individual.

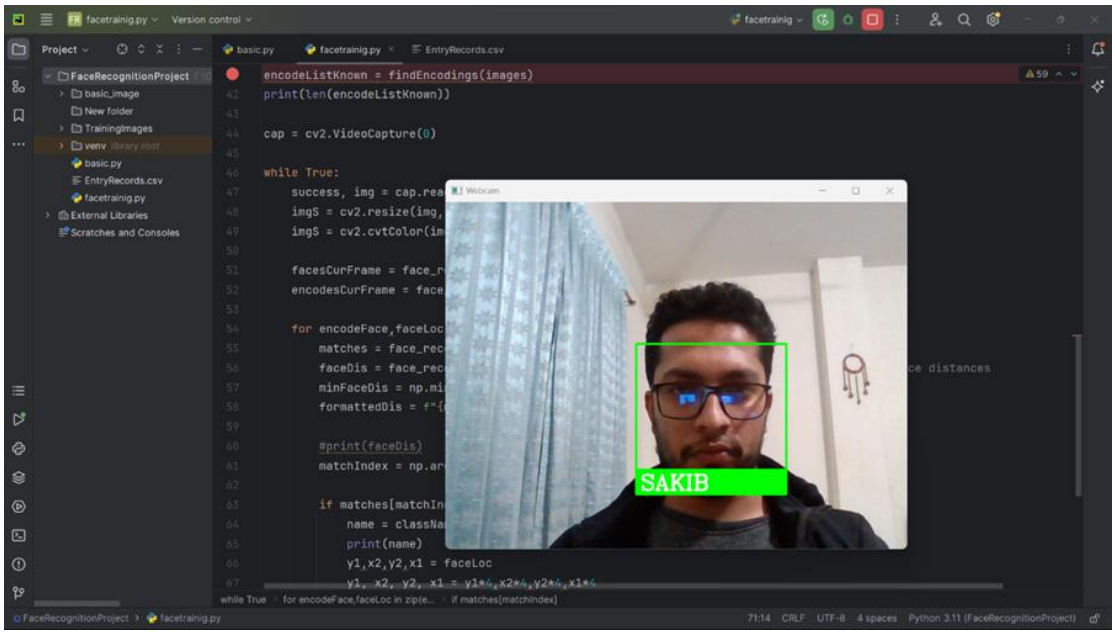


Fig 6.2: Real-time face recognition

REFERENCES

[1] Hangaragi, S., Singh, T., & Neelima N. (2023). Face Detection and Recognition Using Face Mesh and Deep Neural Network. Procedia Computer Science, 218, 741-749.

[2] del Rio, J. S., Moctezuma, D., Conde, C., de Diego, I. M., & Cabello, E. (2016). Automated border control e-gates and facial recognition systems. Computers & Security, 62, 49-72.

[3] Farooq, U., ul Hasan, M., Amar, M., Hanif, A., & Asad, M. U. (2014). RFID based security and access control system. International Journal of Engineering and Technology, 6(4), 309.

[4] Adole, P., Mom, J. M., & Igwue, G. A. (2016). RFID based security access control system with GSM technology. American Journal of Engineering Research, 5(7), 236-242.

[5] Kim, J., Lee, D. & Park, N. CCTV-RFID enabled multifactor authentication model for secure differential level video access control. Multimed Tools Appl 79, 23461–23481 (2020)

[6] Han, B. -J., Jeong, H., & Won, Y. -J. (2011). The privacy protection framework for biometric information in network-based CCTV environment. In 2011 IEEE Conference on Open Systems (pp. 86-90). Langkawi, Malaysia: IEEE.

[7] Zafar, M. R., & Shah, M. A. (2016). Fingerprint authentication and security risks in smart devices. In 2016 22nd International Conference on Automation and Computing (ICAC) (pp. 548-553). Colchester, UK: IEEE.

[8] Pavaloaia, V., & Husac, G. (2022). Tracking Unauthorized Access Using Machine Learning and PCA for Face Recognition Developments. Information, 14(1), 25.

[9] Luma, A. (2015). Real Time Access Control Based on Face Recognition.

[10] Pereira, H., Carreira, R., Pinto, P., & Lopes, S. I. (2020). Hacking the RFID-based Authentication System of a University Campus on a Budget. In 2020 15th Iberian Conference on Information Systems and Technologies (CISTI) (pp. 1-5). Seville, Spain: IEEE.

[11] Alkhurayyif, Y. (2023). Users' Information Security Awareness of Home Closed-Circuit Television Surveillance. Journal of Information Security and Cybercrimes Research, 6(1), 12-23.

[12] Zeki, A. M., Elnour, E. E., Ibrahim, A. A., Haruna, C., & Abdulkareem, S. (2013, November). Automatic interactive security monitoring system. In 2013 International Conference on Research and Innovation in Information Systems (ICRIIS) (pp. 215-220). IEEE.

[13] Costin, A. (2016, October). Security of cctv and video surveillance systems: Threats, vulnerabilities, attacks, and mitigations. In Proceedings of the 6th international workshop on trustworthy embedded devices (pp. 45-54).

[14] Liu, Y., Kong, L., Cao, Y., Sarafian, V., Cheng, L., & Chen, G. (2018). Stop Unauthorized Access to Your Smart Devices. In 2018 IEEE 24th International Conference on Parallel and Distributed Systems (ICPADS) (pp. 228-235). Singapore: IEEE.

[15] Patel, A., Qassim, Q., & Wills, C. (2010). A survey of intrusion detection and prevention systems. Information Management & Computer Security, 18(4), 277-290.

[16] Loos, A., & Ernst, A. (2013). An automated chimpanzee identification system using face detection and recognition. Journal of Image and Video Processing, 49, 2013.

[17] Kalbo, N., Mirsky, Y., Shabtai, A., & Elovici, Y. (2020). The Security of IP-Based Video Surveillance Systems. Sensors, 20(17), 4806.

[18] Scarfone, K., & Mell, P. (2010). Intrusion detection and prevention systems. In Handbook of Information and Communication Security (pp. 177-192). Berlin, Heidelberg: Springer Berlin Heidelberg.

[19] Montero, D. Nieto, M. Leskovsky, P. Aginako, N. Boosting Masked Face Recognition with Multi-Task ArcFace. arXiv 2021, arXiv:2104.09874.

[20] Zhiming Xie, Junjie Li, and Hui Shi. "A Face Recognition Method Based on CNN". Journal of Physics: Conference Series 2019, 1395 012006

[21] Yu-Xin Yang, Chang Wen, Kai Xie, Fang-Qing Wen, Guan-Qun Sheng, Xin-Gong Tang. "Face Recognition Using the SR-CNN Model". Sensors 2018, 18, 4237

[22] Almabdy, S.; Elrefaei, L. Deep Convolutional Neural Network-Based Approaches for Face Recognition. Appl. Sci. 2019, 9, 4397.

[23] Ahsan, M.M.; Li, Y.; Zhang, J.; Ahad, M.T.; Yazdan, M.M.S. Face Recognition in an Unconstrained and Real-Time Environment Using Novel BMC-LBPH Methods Incorporates with DJI Vision Sensor. J. Sens. Actuator Netw. 2020, 9, 54.

[24] Kaggle, available at <<https://www.kaggle.com/datasets/quadeer15sh/lfw-facial-recognition>>, last accessed on 23-10-2023 at 10:00 PM.

[25] Medium, available at << https://medium.com/@ageitgey/machine-learning-is-fun-part-4-modern-face-recognition-with-deep-learning-c3cffc121d78>>, last accessed on 8-11-2023 at 8:00 AM.

REAL-TIME FACE RECOGNITION AND PREVENT UNAUTHORIZED ENTRY ON CAMPUS USING PRE-TRAINED MODELS AND OPENCV

ORIGINALITY REPORT

20%	19%	6%	14%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	dspace.daffodilvarsity.edu.bd:8080 Internet Source	8%
2	Submitted to Daffodil International University Student Paper	2%
3	Submitted to University of Northumbria at Newcastle Student Paper	1%
4	www.mdpi.com Internet Source	1%
5	Submitted to Staffordshire University Student Paper	1%
6	Submitted to Universiti Teknikal Malaysia Melaka Student Paper	<1%
7	ebin.pub Internet Source	<1%
8	Submitted to Indiana University Student Paper	<1%