Arab Academy for Science and Technology and Maritime Transport (AASTMT)

College of Computing and Information Technology
Cairo

B. Sc. Final Year Project

Prison Identification System

[PIS]

Presented by:

Abanoub Medhat

Mohamed Abdelghafar

Mohamed Hani

Nadim Samaha

Ahmed Mostafa

Supervised by:

Dr Mohammed Ragaie

July 2023

Declaration

I hereby certify that this material, which I now submit for assessment on the program of study leading to the award of Bachelor of Science in Computer Science is entirely my own work, and that I have exercised reasonable care to ensure that the work is original, and does not to the best of my knowledge breach any law of copyright, and has not been taken from the work of others save and to the extent that such work has been cited and acknowledged within the text of my work.

Student Name: Abanoub Medhat

Registration No.: 19106340

Signed: ________________________

Date:

Student Name: Mohamed Abdelghafar

Registration No.: 19106314

Signed: ________________________

Date:

Student Name: Mohamed Hani

Registration No.: 18204096

Signed: ________________________

Date:

Student Name: Nadim Samaha

Registration No.: 18204149

Signed: ________________________

Date:

Student Name: Ahmed Mostafa

Registration No.: 18105561

Signed: ________________________

Date:

Acknowledgement

The authors would like to express their gratitude to all those who contributed to this research project. We would like to thank the staff at our college for their cooperation and participation in this valuable journey. We would also like to thank our colleagues for their valuable feedback and support throughout the development and implementation of the system. In addition, we would like to acknowledge the support and resources provided by the team members. Finally, we would like to express our appreciation to the anonymous reviewers for their constructive comments and suggestions that helped improve this project's quality.

Abstract

This document describes the design and implementation of a face recognition system for use in prison facilities. The system is intended to improve prison security and efficiency by identifying inmates and staff members.

The system provides security for all types of indoor and outdoor prison facilities, to enable guards to monitor and track inmates, detect illegal activities, isolate, and control violent incidents, and prevent intrusion into confidential areas inside the prison. Then store these data in a database.

The system is intended to safeguard any prison facility from any danger or illegal activities. Create an integrated, easy-to-use interface. So, new employees can be trained to use our platform in a matter of days. Report immediately to the security department if any danger occurs.

It is used for security purposes to improve overall safety by viewing the entire facility on one screen.

It is intended for Improving Prison Security. Monitor, Control, & Track prisoners from causing any illegal activities inside the prison facilities.

The results of this study suggest that the face recognition system has the ability and potential to improve the security and efficiency of prison operations, enhancing safety for both inmates and staff members.

Keywords: Face Recognition, Face Detection, Security, Prison Facilities, Artificial Intelligence, Computer Vision, Machine Learning, Deep Learning, Image Processing, OpenCV.

Contents

Chapter I: Proposal (General Introduction)

Description

It is a system that provides security for all types of indoor and outdoor prison facilities, to enable guards to monitor and track inmates, detect illegal activities, isolate, and control violent incidents, and prevent intrusion into confidential areas in the prison. Then store these data in a database.

It is used for **security** purposes to improve overall safety by viewing your entire facility on one screen.

The main objective & priority is to improve security systems and save prisons from disturbance, trouble, or any illegal activities.

Problems

- How to know if prisoners had entered their cells on time?
- How to make sure that the prisoners did not cause any illegal activities?

Solution

- The system verifies whether the prisoner has entered his cell on time or did cause any illegal activities by tracking each step he takes, alerting the guards and facing severe circumstances if he did not follow the prison’s rules.

Components Used

- Webcam 720p
- Laptop
- Flask framework & OpenCV library in Python (using MS Visual Studio Code)
- MySQL Database (using PhpMyAdmin + Wamp Server)

Recommended Components

- 4K CCTV Camera with night vision & smart tracking sensors
- Computers and servers with advanced hardware & infrastructure
- Ultra-Fast Internet speed *(1 GB/S at least)*
- Large Datasets *(contains millions of images of faces)*
- Oracle Database
- Highly Skilled personnel with expertise in machine learning, computer vision, and computer security

Chapter II: Literature Review

Introduction

Images are important in today's information age. There are a thousand words in a picture. They are created quickly and are widely dispersed. One explanation for all of this is the availability and affordability of cameras and other photographic equipment. Thanks to image retrieval tools like Google's image search, it is now feasible to swiftly search for photos using keywords. However, it is difficult to make the computer understand the semantics present in images. Simply explained, this is a result of the computer's failure to understand the context. It can be very challenging to compare and recognise faces in photos.

Researchers have explored automatic facial recognition systems for more than 60 years. The first psychological paper to examine face recognition was published in the 1950s. In 1970, Kelly finished the first study on automatic facial recognition. In his dissertation, he describes a computer programme that handles a difficult image-processing task. The task was to locate the same person among a collection of pictures taken by a TV camera.

Face recognition is a topic that interests many different research fields, not only computer scientists. Even though it all began with psychologists, a significant amount of research has been done over the past 40 years by psychophysicists, neuroscientists, and other engineers. Whether or not the perception of faces is a particular mechanism is one of the problems that neuroscientists and psychophysicists have been interested in. There is ongoing debate surrounding this subject among psychologists.

The face recognition field made no development in the 1980s. However, interest surged quickly once more during the start of the 1990s, which provides some explanations for why research interest increased: real-time hardware became more accessible, and the significance of applications connected to surveillance increased.

Main Body

Approach

The practice of recognizing, confirming, or verifying a person's identification by their face is known as **FRT** – Facial Recognition Technology. FRT uses a person's facial details to capture, analyze, and compare patterns. It operates by using algorithms in the manner described below, in simple terms:

Step 1: Find faces in person, pictures, or videos.

Step 2: Converting a face's analogue information into a set of usable digital data depending on the person's facial traits.

Step 3: Using the digital data gathered, compare two photographs to make sure they match.

Over the past few years, FRT utilization in the workplace has expanded, and it is currently utilized in a variety of professional contexts.

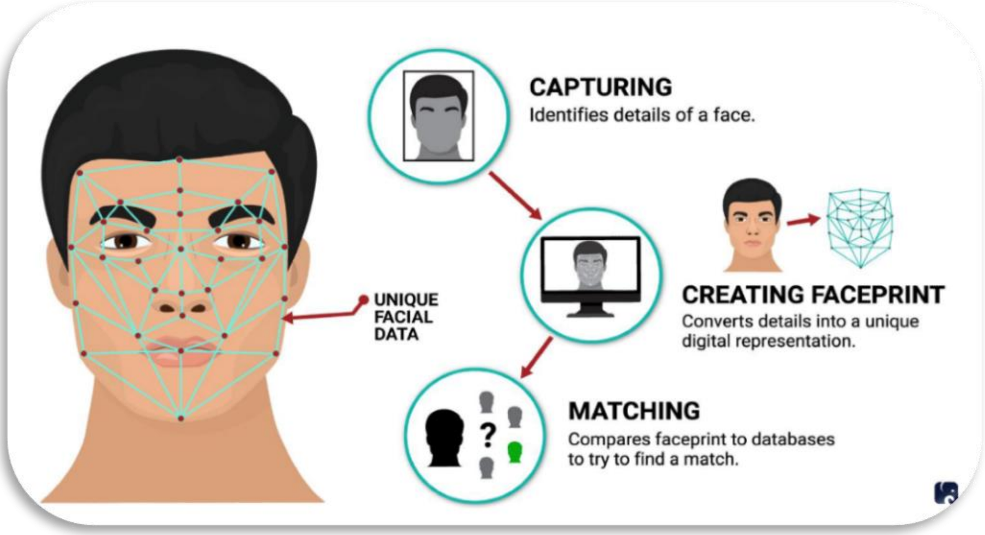
Traditional clock-in/time recording, verification, and monitoring systems are open to abuse, particularly in places where a lot of people routinely come and go. FRT was introduced early in some industries, including manufacturing and construction, where it might be difficult to track accurate on-site detection and where the practice of employees reporting in for missing teammates may be troublesome. It has also seen an expansion in other industries in recent years.

The software often calls for the employee to enter a special pin code and then stand in front of a camera while FRT verifies their identity.

When employees enter and leave the office or certain areas of the workplace, FRT is increasingly utilized to manage access and confirm their identities. Businesses, organizations, and facilities are using FRT more regularly to assist with compliance and security requirements. It should not be surprising that this occurs more frequently in sectors with strict regulations, such as the financial services sector, where companies are required to follow rigid compliance guidelines.

The general approach for a face recognition system involves several steps, including:

- Face Detection
- Face Alignment
- Feature Extraction
- Face Matching
- Face Recognition


CAPTURING
Identifies details of a face.
UNIQUE FACIAL DATA
CREATING FACEPRINT
Converts details into a unique digital representation.
?
MATCHING
Compares faceprint to databases to try to find a match.

The **main issues** with FRT are:

- Not accurate enough
  - To ensure high efficiency & precision, the system needs to be trained with hundreds of thousands of images with high quality.

- Some Latency & Delays
  - To minimize delays, the system needs powerful hardware and servers with advanced features & technology.
- Few Personnel
  - To provide constant stability, high performance and continuous maintenance, The system needs highly skilled and professional people with at least 7 years of experience in AI, Machine Learning and Computer Vision.
- Difficulty in detecting people wearing (masks, hats, scarves, etc.)
- Low-Quality Image *[shaky/blurry image]*

- Privacy Breach *(privacy violation)*
- Bias *(favouritism)*
- Discrimination *(racism)*

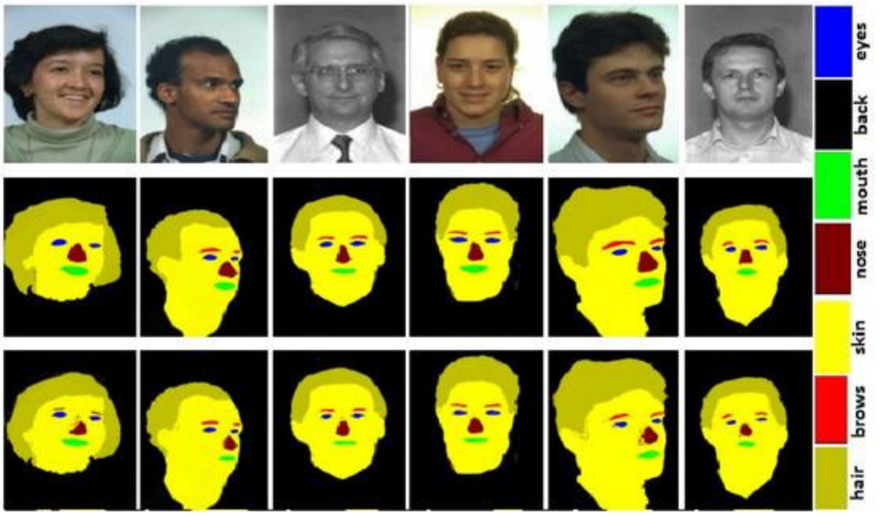
Two of the key issues with the use of FRT are its accuracy and the possibility of algorithmic racial or sexual bias. The Equality and Human Rights Commission highlighted evidence indicating that several automatic FRT algorithms disproportionately misidentify black people and women, increasing the prospect of discrimination, in its report to the UN on civil and political rights in the UK.

If an employer bases choices wholly or mostly on FRT data, the employer may be the target of a discrimination claim (for example, to deny employment opportunities, or to discipline or dismiss an employee accused of disciplinary breaches, poor performance, or absence identified primarily using FRT). The amount of money awarded for successful discrimination lawsuits is uncapped, and because such cases are almost always high-profile and generate internal gossip as well as media attention, employers should carefully assess the dangers involved.

Methods & Techniques

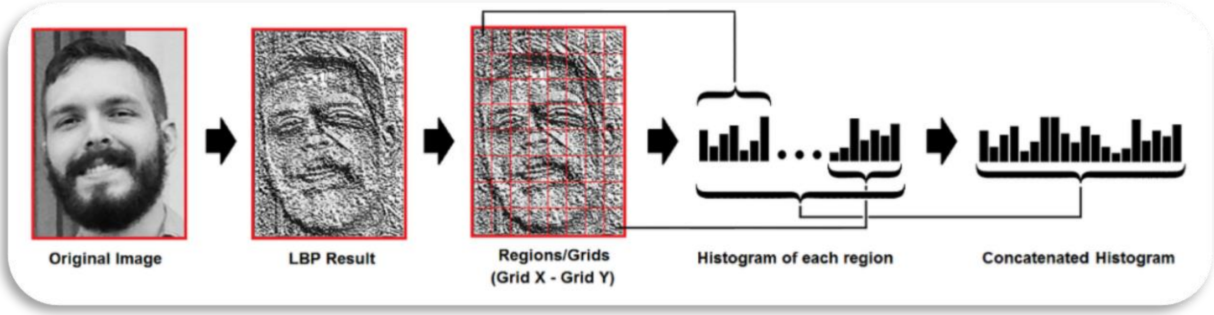
There are several techniques used in face recognition. These techniques can be used in combination with each other to improve the accuracy & efficiency of the face recognition system. Some of them are:

- Local Binary Patterns Histograms (LBPH) ***“The one we’ve used”***
- Deep Learning *[such as Convolutional Neural Networks (CNNs)]*
- Viola-Jones
- Eigenfaces *[using Principal Component Analysis (PCA)]*
- Fisherfaces *[using Linear Discriminant Analysis (LDA)]*
- Local Feature Descriptors *[such as “SIFT” & “SURF”]*



1. Local Binary Patterns Histograms (LBPH)

- LBPH is a texture analysis algorithm that can be used to extract features from a face image. It works by comparing the intensity values of neighbouring pixels and encoding the results into a binary pattern.



The reason for choosing this technique:

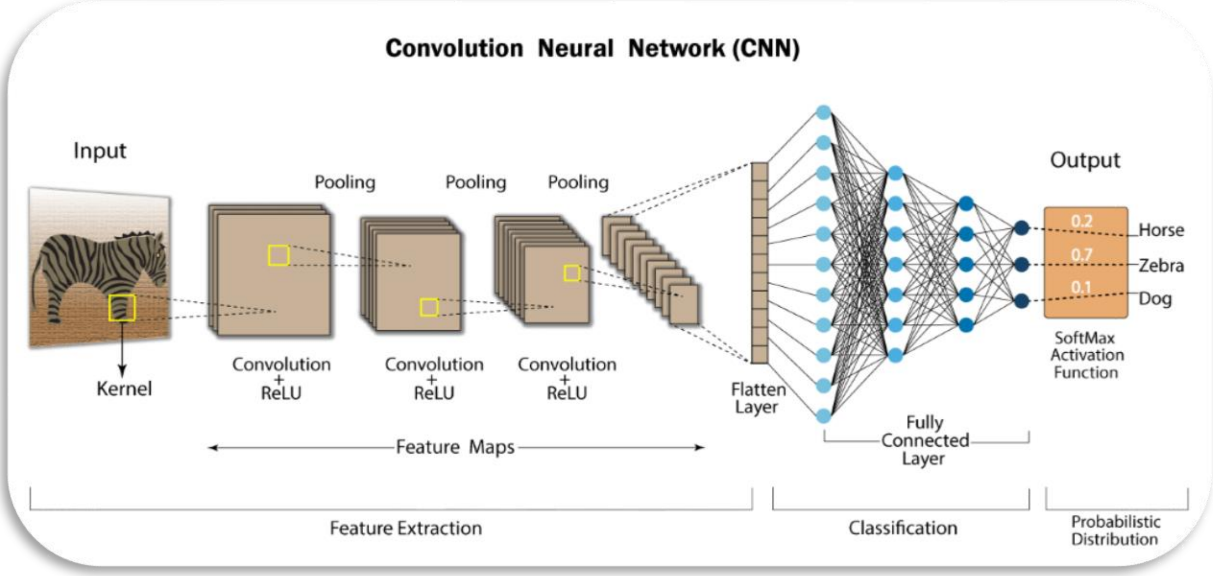
1. **Good Performance on Small Datasets:** The LBP Histogram algorithm can perform well even on small datasets, making it useful for applications where only a limited number of face images are available for training.
2. **Simple Implementation:** The LBP Histogram algorithm is relatively simple to implement and does not require complex neural networks or deep learning techniques. This can make it easier to understand and modify for specific applications.
3. **Insensitivity to Facial Expression and Pose:** The LBP Histogram algorithm is relatively insensitive to changes in facial expression and pose, which can be important for face recognition systems that need to operate under varying conditions.
4. **Computational Efficiency:** The LBP Histogram algorithm is computationally efficient and can be calculated quickly, making it suitable for real-time face recognition applications.
5. **Robustness to Illumination Variations:** The LBP Histogram algorithm is robust (solid/strong) to illumination (lighting) variations in face images. This is because the LBP operator encodes the texture information of an image, which is less affected by illumination changes than colour or intensity information.

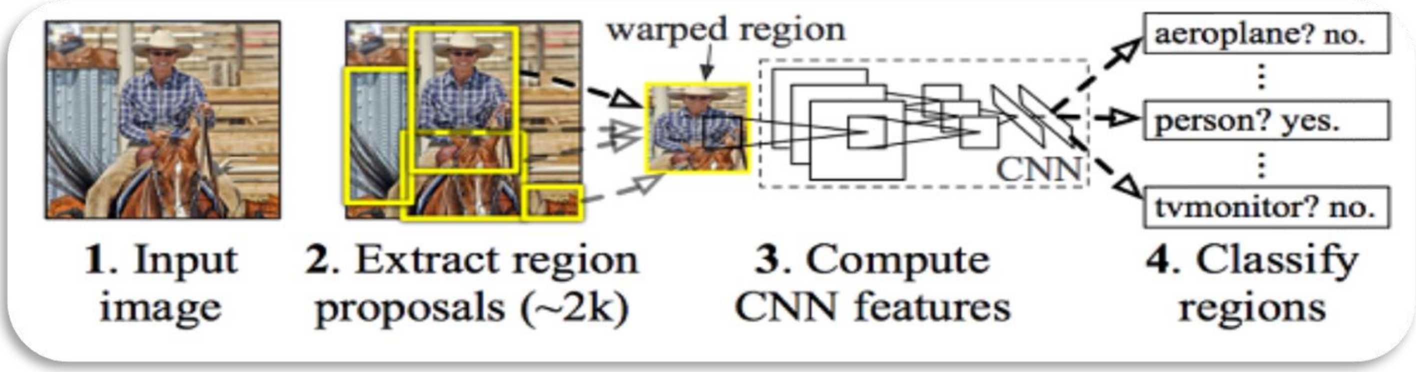
Related Work

2. Deep Learning

- Deep learning techniques, such as Convolutional Neural Networks (CNNs), can be used to extract features from a face image. These techniques have been shown to achieve state-of-the-art performance in face recognition tasks by learning to automatically extract discriminative features from the input image.

- **CNN** is considered to be one of the best and most powerful tools in object detection, computer vision and machine learning. It is widely used by the top companies in the technology industry like Amazon, Google, Microsoft, Meta, and Apple. But one of the disadvantages is that it needs millions of dataset images for the detection process.





3. Viola-Jones

Basic Idea

- Takes a bunch of faces as data.

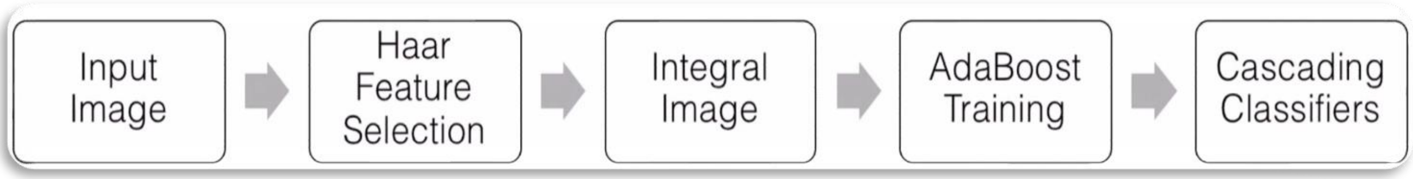
- Hard-code the feature of the face
- Train the program to feature the set of faces

Advantages

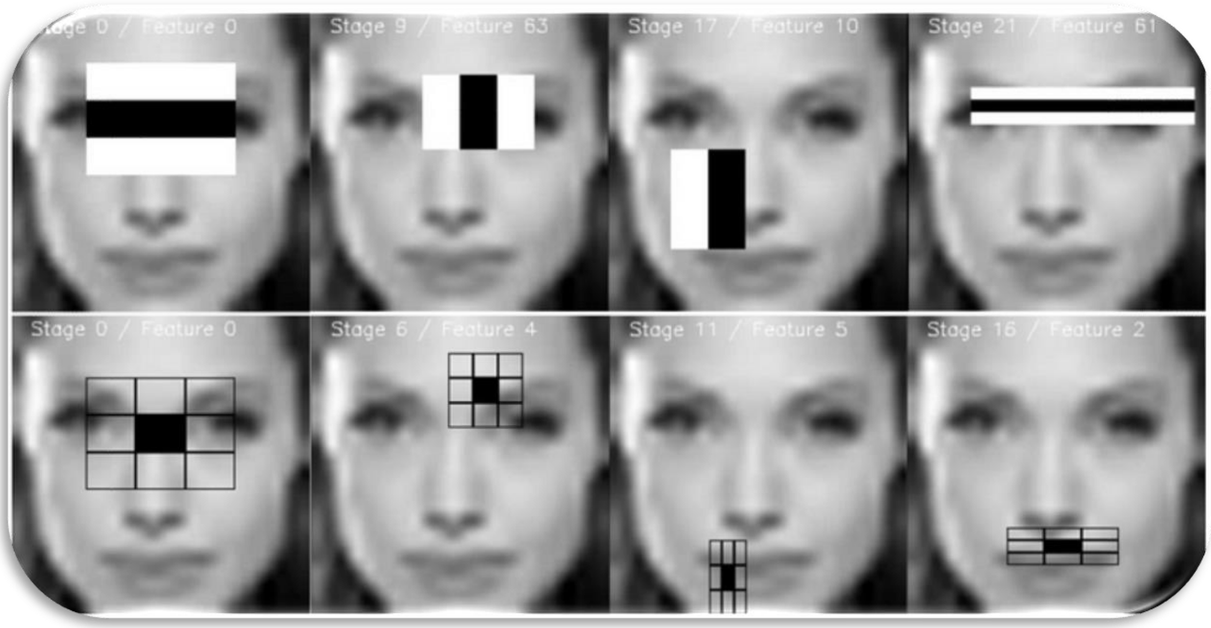
- So **powerful** that “Apple” and “Snapchat” used this algorithm
- **Fast**: Real-time Processing
- **Robust** *(very accurate & precise)*: High correction detection rate

Disadvantages

- Cannot detect faces if they are tilted/rotated or shaky.
- Sensitive to light conditions.



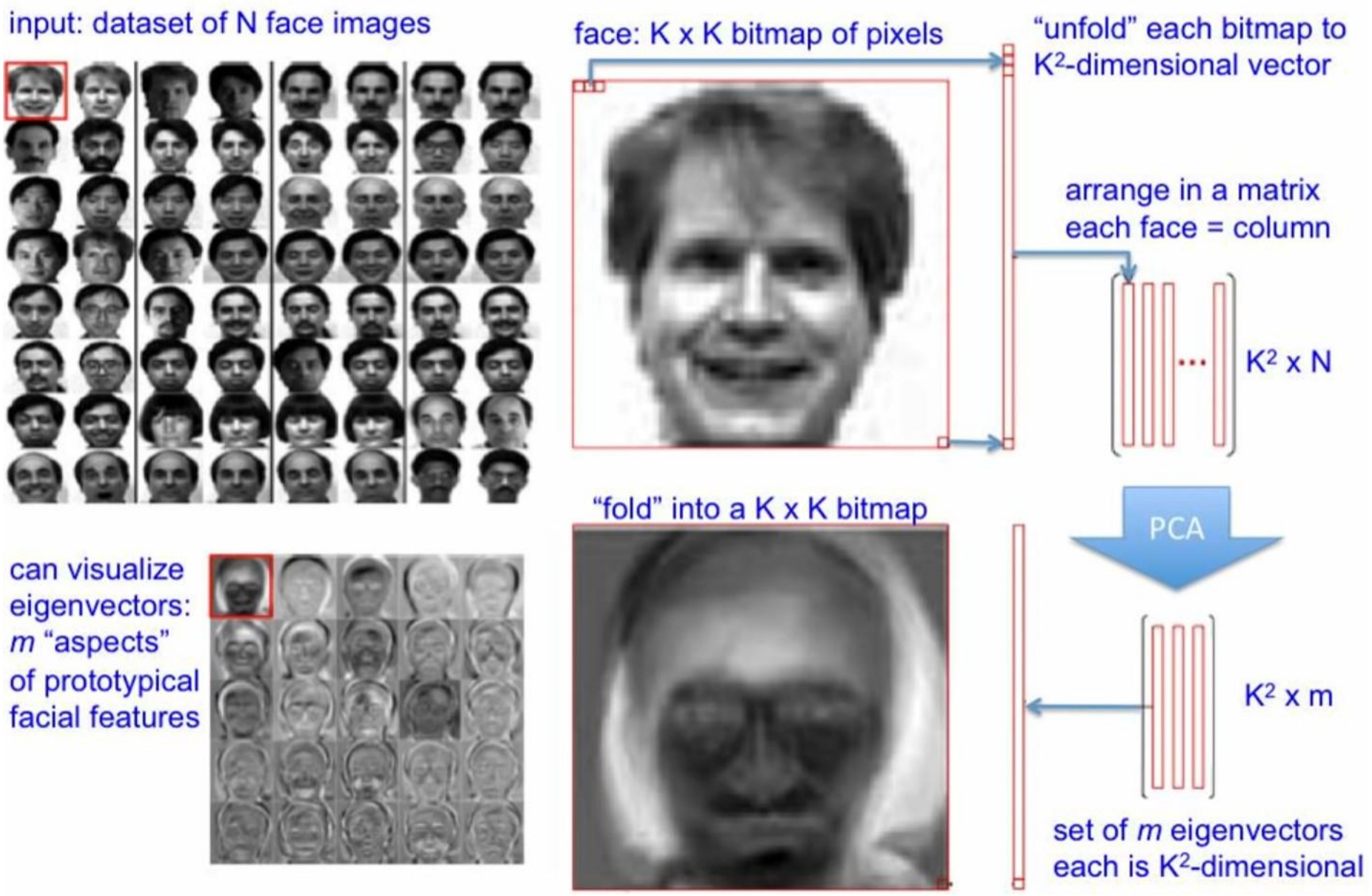
Input Image → Haar Feature Selection → Integral Image → AdaBoost Training → Cascading Classifiers



4. Eigenfaces

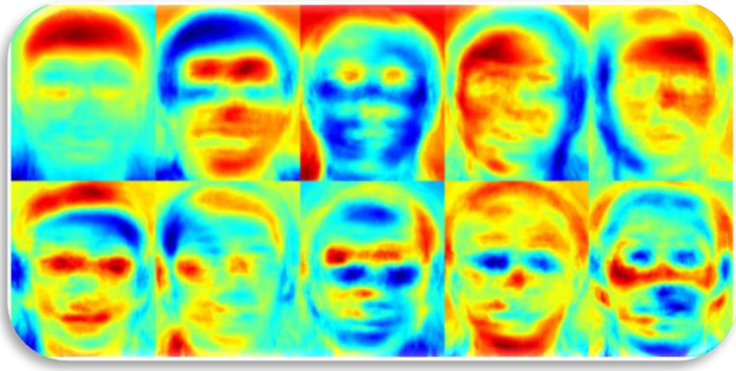
- This approach covers face recognition as a two-dimensional recognition problem.

- A technique that uses principal component analysis (PCA) to extract features from a face image. It works by representing each face as a linear combination of a set of eigenfaces, which are the principal components of the face space.


input: dataset of N face images
face: K x K bitmap of pixels
"unfold" each bitmap to K²-dimensional vector
arrange in a matrix
each face = column
K² x N
PCA
K² x m
set of *m* eigenvectors
each is K²-dimensional
"fold" into a K x K bitmap
can visualize eigenvectors: *m* "aspects" of prototypical facial features

5. Fisherfaces

- Fisherfaces is a technique that uses linear discriminant analysis (LDA) to extract features from a face image. It works by finding a set of discriminant vectors that maximize the separation between different classes of faces.



Some other approaches that can be used as well, including:

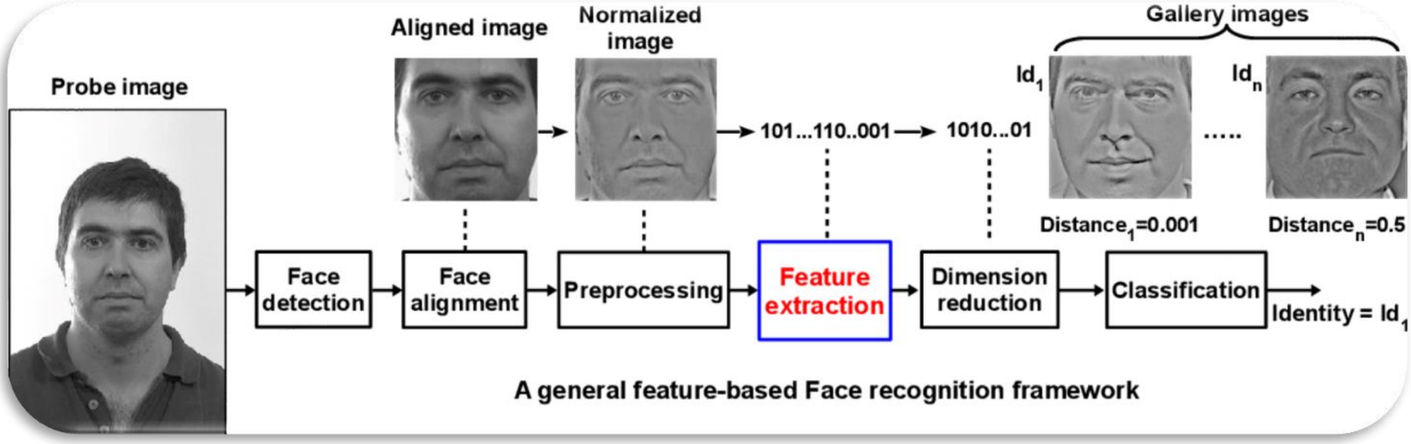
- Feature-based
- Model-based
- Hybrid Method

Feature-based

Local features like the eyes, nose, and mouth are first extracted, and the structural classifier is then given information about their position, shape, and appearance. The "recovery" of features when the system tries to retrieve features that are not visible due to significant fluctuations is a problem for feature extraction methods. To make a head position, combine the front and profile pictures.

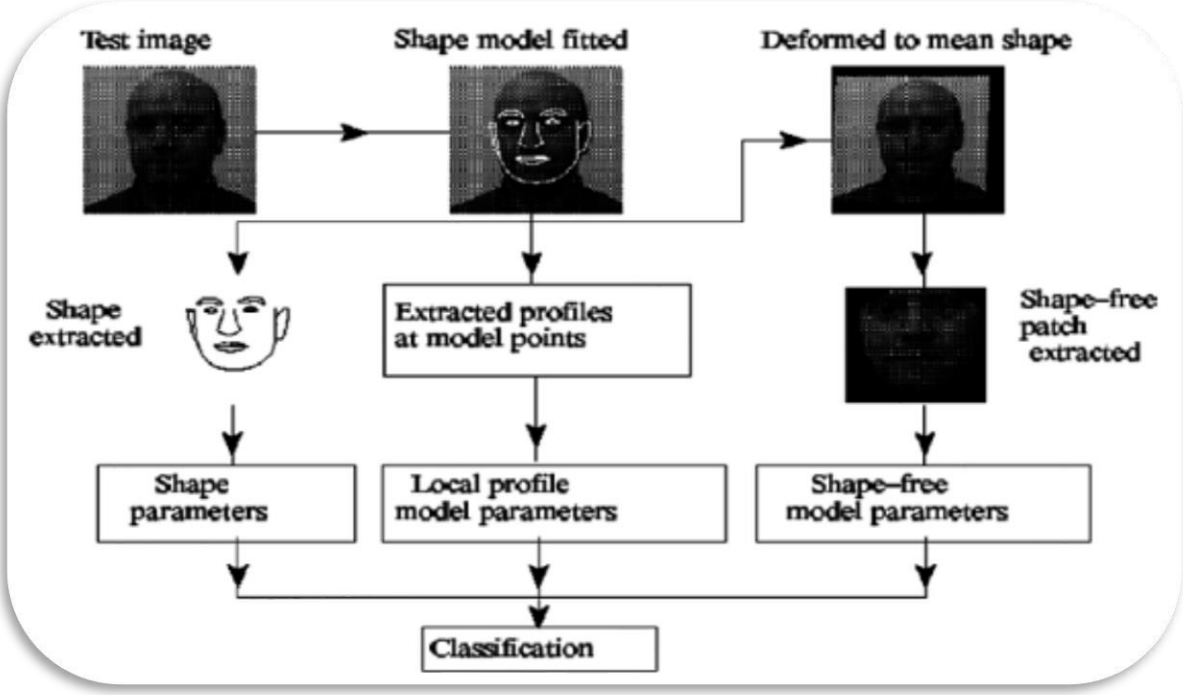
Different extraction methods:

- Generic methods based on edges, lines, and curves.
- Feature-template-based methods.
- Structural matching methods.



Model-Based

A face is modelled using the model-based technique. The model is given the new sample, and the model's parameters are then utilised to identify the image. A model-based approach can be categorised as 2D or 3D.


Test image
Shape model fitted
Deformed to mean shape
Shape extracted
Extracted profiles at model points
Shape-free patch extracted
Shape parameters
Local profile model parameters
Shape-free model parameters
Classification

Hybrid Approach

It combines holistic and feature extraction methodologies. These techniques frequently employ 3D pictures. Take a 3D picture of your face and study the contours of your forehead, jaw, and eye sockets. The method gives enough data to generate the full face using the depth and measurement axes, therefore a profile face is also adequate. Detection, localization, measurement, representation, and mapping are all included in 3D systems.

- **Detection** - Capturing a face by scanning a photograph or photographing a person's face in real-time.
- **Position** - Determining the location, size, and angle of the head. Assign measurements to each curve of the face to make a template.
- **Representation** - Converting the template into a numerical representation of the face.

- **Matching** - Comparing the received data with faces in the database. The 3D image which is to be compared with an existing 3D image needs to have no alterations.

Related Systems

• Amazon Rekognition	*[https://aws.amazon.com/rekognition/]*
• BioID	*[https://www.bioid.com/]*
• Cognitec	*[https://www.cognitec.com/]*
• Paravision	*[https://www.paravision.ai/]*

Datasets

Each user is trained for 10 images using the “Haar Cascade” Classifier. The images are then stored in a folder named “dataset”, and then the database (PhpMyAdmin) takes the folder “dataset” as a reference. Therefore, the dataset is stored inside the system not the database; to improve performance & efficiency.

The model is trained from 1,012 face images located inside a folder named “training” using the Linear Binary Patterns Histograms (LBPH) technique which is inside the OpenCV library. We used this technique specifically because of its:

- Good performance
- Efficiency
- Simplicity to implement

Libraries, Frameworks and Classifiers

The libraries, frameworks, and classifiers that have been used in Python for our system are:

- Flask framework *(with HTML, CSS, JavaScript)*
    - ➢ Used to create the web application in Python.
- OpenCV library
    - ➢ Linear Binary Patterns Histograms (LBPH) Technique
        - o A simple grayscale texture analysis algorithm that can be used to extract features from a face image.
    - ➢ Haar Cascade Algorithm (a Cascade Classifier)
        - o Used to detect faces quickly and in real-time.
    - ➢ Trained Algorithm (a train classifier)
        - o A Neural Network model trained on image datasets to improve face recognition accuracy & efficiency.
- NumPy library
    - ➢ Used to process & load the arrays of images used for the facial recognition training

Conclusion

One of the most effective techniques currently being developed is facial recognition technology. Businesses and organisations like (Malls, Hypermarkets, Prisons, …) benefit greatly from the effort, time, and cost savings. It enhances the security systems for organizations. It ensures the rights of the workforce. The eigenface method developed by Turk and Pentland was the most successful and effective method and strategy utilised for facial recognition systems. A system with intelligence should be able to change over time. To learn and subsequently recognise new faces in an unsupervised way, one can reason about images in face space. A picture is originally categorised as "unknown" if it is sufficiently close to face space (face-like), but not one of the recognised faces. The unknown image and the pattern vector are both stored on the computer. The existence of a novel but the unidentified face is hypothesised if a group of "unknown" pattern vectors cluster in the pattern space. Since the system primarily uses an auto-associative memory for the recognised faces, recognition performance ought to decline gradually in the presence of a noisy image or a partially obscured face. The projection of the obstructed face image serves as proof of this.

Software Requirements Specification (SRS)

Introduction

It is a system that provides security for all types of indoor and outdoor prison facilities, to enable guards to monitor and track inmates, detect illegal activities, isolate, and control violent incidents, and prevent intrusion into confidential areas inside the prison. Then store these data in a database.

The system safeguards any prison facility from any danger or illegal activities. So, How to know if the prisoner has entered his cell on time? How to make sure that the prisoner did not cause any illegal activities? By tracking each step, he takes, alerting the guards and facing severe circumstances if he did not follow the prison’s rules.

Purpose

The main purpose is to enhance **security** and improve the accuracy & efficiency of the identification process by controlling & observing the entire prison from only one room using the system.

This is done by using:

- **Access Control** [To verify the identity of individuals, access can be granted or denied automatically, without the need for human intervention to reduce the risk of unauthorized access to any secure area/building]
- **Surveillance** [To identify and track individuals who may pose a security threat. By analyzing a video stream from surveillance cameras and matching the faces of individuals against a watchlist or database of known individuals, security personnel can be alerted to potential threats in real time]
- **Law Enforcement** [To quickly & accurately identify potential suspects or wanted individuals and compare their faces against a database of known criminals]
- **Border Control** [To verify the identity of the criminals and ensure that they did not pass the prison borders]

Intended Audience

It is intended for:

- **Prison facilities:** that need more security & verification to control, monitor, & track their prisoners effectively.
- **Administrative/Operation Prison Officers:** will be the system users.

Intended Use

The system's intention is to be used for:

- Improve Prison Security.
- Monitor, Control, & Track prisoners from causing any illegal activities inside the prison facilities.

Scope

Our main objective & priority is to improve security systems and save prisons from disturbance, trouble, or any illegal activities.

Definitions

System

A verification system that provides security for all types of indoor and outdoor prison facilities, to enable guards to monitor and track inmates, detect illegal activities, isolate, and control violent incidents, and prevent intrusion into confidential areas in the prison. Then store these data in a database.

Features & Functionality

- Highly Practical
- Cost-effective
- Safe

- Simple
- Eco-friendly
- HD Camera
- Minimum Complexity
- Easy to deploy

Challenges & Risks

- Limited capabilities & coverages
- Could be hacked – *nothing is 100% secured*
- System errors & bugs
- Limited Budget

Mitigate Risks

- Provide high network coverage with very fast internet.
- Provide CCTV ultra-HD\4K camera with 60 fps and night vision & smart tracking sensors *(more expensive)*.
- Continuous system maintenance & testing.

Chapter III: Methodology

Data Collection is the first step to collecting a dataset of images that will be used to train and test the face recognition system. The system needs hundreds of thousands of images, and they should be of high quality and have consistent lighting, pose, and expression. **Face Detection** is the next step to use a face detection algorithm to identify and locate faces in the input images *(OpenCV in Python)*. **Face Alignment** is the third step once the faces have been detected to align them to a common reference frame. This is necessary to ensure that the facial features are in a consistent position and scale, which can improve the accuracy of the recognition algorithm *(i.e., fix faces if they're blurred or tilted)*. **Feature Extraction** is the fourth step to extract the facial features from the aligned faces. **Face Matching** is the final step to use the extracted facial features to match the input face to a known identity.

System Description

User Requirements

The system should be easy and simple to operate and interact with. It should have an integrated, easy-to-use interface. So, new employees can be trained to use the system in a matter of days.

The system should have “Access Control” to display names and photos of users entering doors.

The system should monitor, observe, and control any type of doors and gates inside the prison facilities.

The system should be fast, can synchronize with the camera effectively, and have a quick response.

The system should integrate with the prison Alerting system to alarm guards **who** caused any illegal activities, violent incidents, or aggressive intrusions inside the prison facilities.

Assumptions and Dependencies

We assume that system users “Administrative / Operation Officers” inside the prison facilities have a basic level of computer knowledge.

We assume that prison facilities have fast internet speed, stable network connection, and advanced computers that can handle the system properly.

We assume users with administrative access are careful in deleting or modifying any information knowingly or unknowingly which will lead to inconsistency in the database.

Constraints and limitations

- **Language:** The interface is only in English; no other language option is available.
- **Occlusions** ***(Obstacles)*****:** Face recognition systems can be impacted by occlusions, such as glasses, hats, scarves, and masks that partially cover or obscure the face. This can make it difficult for the system to accurately recognize faces.
- **Age & Gender:** Face recognition systems can be less accurate when recognizing the faces of young children or older adults.
- **Pose & Lighting Variations:** Face recognition systems can struggle to recognize faces that are not in a standard pose, such as faces that are tilted or turned away from the camera or any changes in the illumination conditions of the face.

Intended Technology

Facial recognition technology involves a combination of computer vision and machine learning techniques. some of the key technologies used in facial recognition are:

1. **Face Detection Algorithms** *[To locate & extract faces from an image or video stream, such as Haar cascades and Convolutional Neural Networks (CNNs)]*.
2. **Face Alignment Algorithms** *[To normalize the face's pose & scale, which can help to improve the accuracy of the feature extraction and feature matching algorithms, such as the Iterative Closest Point (ICP) algorithm]*.
3. **Feature Extraction Algorithms** *[To extract meaningful features from the face image, such as Local Binary Patterns (LBP) and Eigenfaces]*.
4. **Feature Matching Algorithms** *[To compare the features extracted from the input face with those of known faces in a database. This can be done using traditional machine learning algorithms, such as k-Nearest Neighbors (k-NN) and Support Vector Machines (SVMs)]*.

5. **3D Facial Recognition Technologies** *[Use depth sensors/cameras to capture the facial geometry and create a 3D model of the face]*.

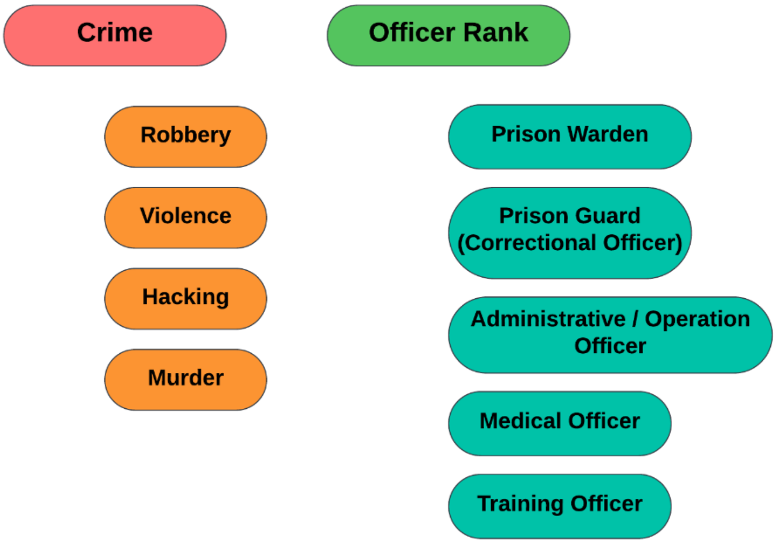
Application Description *“System Interface”*

The system starts by showing the “Index Page” (Main Page) that shows the personnel’s data and two buttons: “Add Personnel button*” [which adds another person inside the system database]* and “Face Recognition button” *[which recognizes faces in a video stream using the external camera]*.

Once we click the first button “Add Personnel button”, it navigates to the “Add Personnel Page” which consists of:

- ID *[which is inserted automatically]*
- Name *[Enter the name of the required person]*
- Crime/Officer Rank *[Select the Crime/Officer Rank of this person]*
- “Next” button *[To navigate to the “Generate Dataset Page” for Face Training]*
- “Back” button *[To return to the “Index Page”]*

The second button “Face Recognition button” navigates to the “Face Recognition Page” which shows a real-time video stream that recognizes faces and records it in “Today Scan”.



System Requirements

Functional requirements

It describes what the system should do, including:

1. **Face detection:** The system should be able to detect faces from an input image or video stream. This may involve using computer vision techniques such as Haar cascades, Viola-Jones algorithm, or deep neural networks.

2. **Feature extraction:** The system should be able to extract facial features from the detected faces. This may involve using techniques such as Local Binary Patterns (LBP), Histogram of Oriented Gradients (HOG), or deep neural networks.

3. **Face matching:** The system should be able to compare the extracted features of a detected face with the features of faces in a database to determine if there is a match. This may involve using techniques such as Euclidean distance, cosine similarity, or deep metric learning.

4. **Face recognition:** The system should be able to recognize the identity of a detected face by matching its features with those of known individuals in a database. This may involve using techniques such as one-to-one or one-to-many matching.

5. **User interface:** The system should have a user-friendly interface that allows users to interact with it.

6. **Privacy and security:** The system should ensure the privacy and security of the data it processes. This may involve using encryption techniques, access control mechanisms, or other security measures to protect the system from unauthorized access or misuse.

7. **Performance:** The system should be able to process input data in a timely and efficient manner, with low latency and high accuracy through optimizing the algorithms used for face

detection, feature extraction, and face matching, and using advanced hardware.

Non-Functional requirements

It describes the requirements that are not directly concerned with the specific functions delivered by the system, including:

- **Usability:** The system is user-friendly, with a simple and intuitive interface that is easy to use.
- **Maintainability:** The system is constantly maintained by handling any problems, bugs, or errors that occur suddenly.
- **Safety & Availability:** The system is safe and available to use.
- **Reliability:** The system is reliable with minimum disruptions.

System Verification

- The system user must fill out all required fields. If a field is blank, a popup message will appear saying *"Please fill out this field"*. And the user can't continue to the next step.
- The trainee must appear physically in front of the system camera. A printed image can not be used for the facial recognition process.

System Validation

System validation is a crucial step to ensure the accuracy, reliability, and fairness of the system. However, it is affected by multiple conditions, including:

1. **Performance Evaluation** *[The performance of the system should be evaluated under a range of conditions, such as variations in lighting, pose, and occlusions]*
2. **Testing** *[The system should be tested on a diverse dataset of face images, including images of individuals with different facial features]*

3. **Ethical Considerations** *[The system should be evaluated for potential ethical concerns, such as data privacy, and developing policies and procedures to address these concerns]*

4. **Integration & Deployment** *[The system should be integrated with multiple systems including Alarm System, Fire Department System, and Medical System]*

System Features

Verify Prisoner

- **Function:** Verify the prisoner manually and show his credentials
- **Priority:** Top (1st release)
- **Requirements:** Prisoner's ID

Add Prisoner

- **Function**: Sign up a new prisoner to the system
- **Priority**: Top (1st release)
- **Requirements**: Prisoner's data (Id, Name, Personal ID, Gender, Age, Phone no, Crime, …)

Update Prisoner

- **Function**: Update prisoners' information on the system
- **Priority**: Top (2nd release)
- **Requirements**: Prisoner's data (Id, Name, Personal ID, Gender, Age, Phone no, Crime, …)

Delete Prisoner

- **Function**: Delete prisoner record from the system
- **Priority**: Top (2nd release)
- **Requirements**: Prisoner's data (Id, Name, Personal ID, Gender, Age, Phone no, Crime, …)

Alert Security Department

- **Function**: Alert the security department if any illegal activity occurs inside the prison
- **Priority**: Medium (2nd release)
- **Requirements**: Check for any violent incidents, aggressive intrusions, or accessing confidential areas inside the prison.

Prisoner Report

- **Function**: Show the prisoner's status and his behaviour every month.
- **Priority**: Low (3rd release)
- **Requirements**: Prisoner's data each month

Emergency

- **Function**: Connect to the Fire, Police, or Medical departments
- **Priority**: Medium (2nd release)
- **Requirements**: An emergency happens like (fire, crime, or health issues) inside the prison

Voice Recognition

- **Function**: A premium feature used for extra security in the Top-level or Top-secret areas inside the prison facilities.
- **Priority**: Top *(2nd release)*
- **Requirements**: Top-level or Top-secret areas inside prison facilities

Chapter IV: Implementation

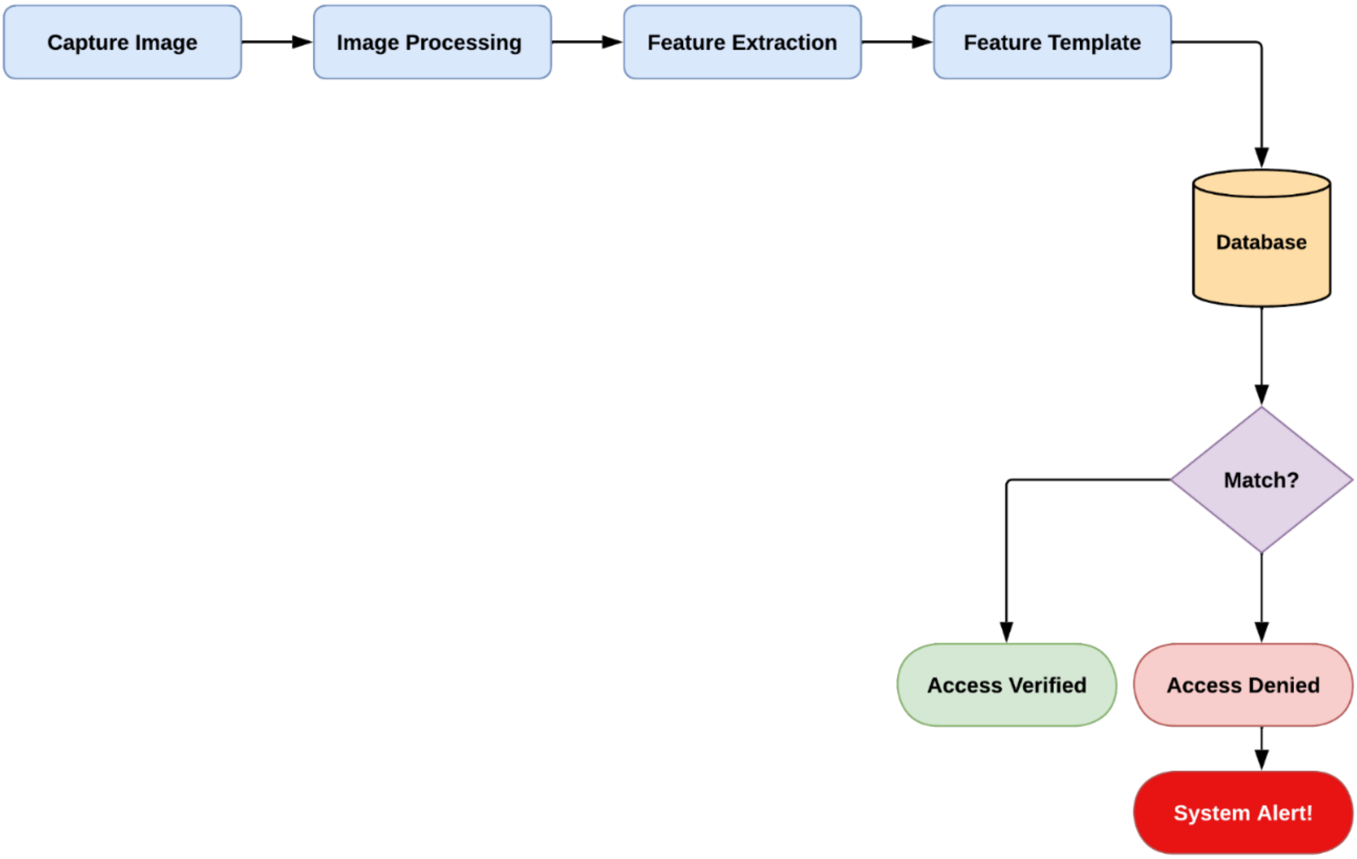
In this study, we implemented a face recognition system using a Linear Binary Patterns Histograms (LBPH) architecture. The system was trained on a dataset of 1,012 face images, including variations in lighting, pose, and facial expression. We used Flask framework to create a web application in Python. We used NumPy library to process & load the arrays of images used for the facial recognition training. We used OpenCV library to gain access to the Linear Binary Patterns (LBP) technique, the Haar Cascade Classifier Algorithm, and the train classifier Algorithm. Then store the face recognition images in a database.

Software Design Document (SDD)

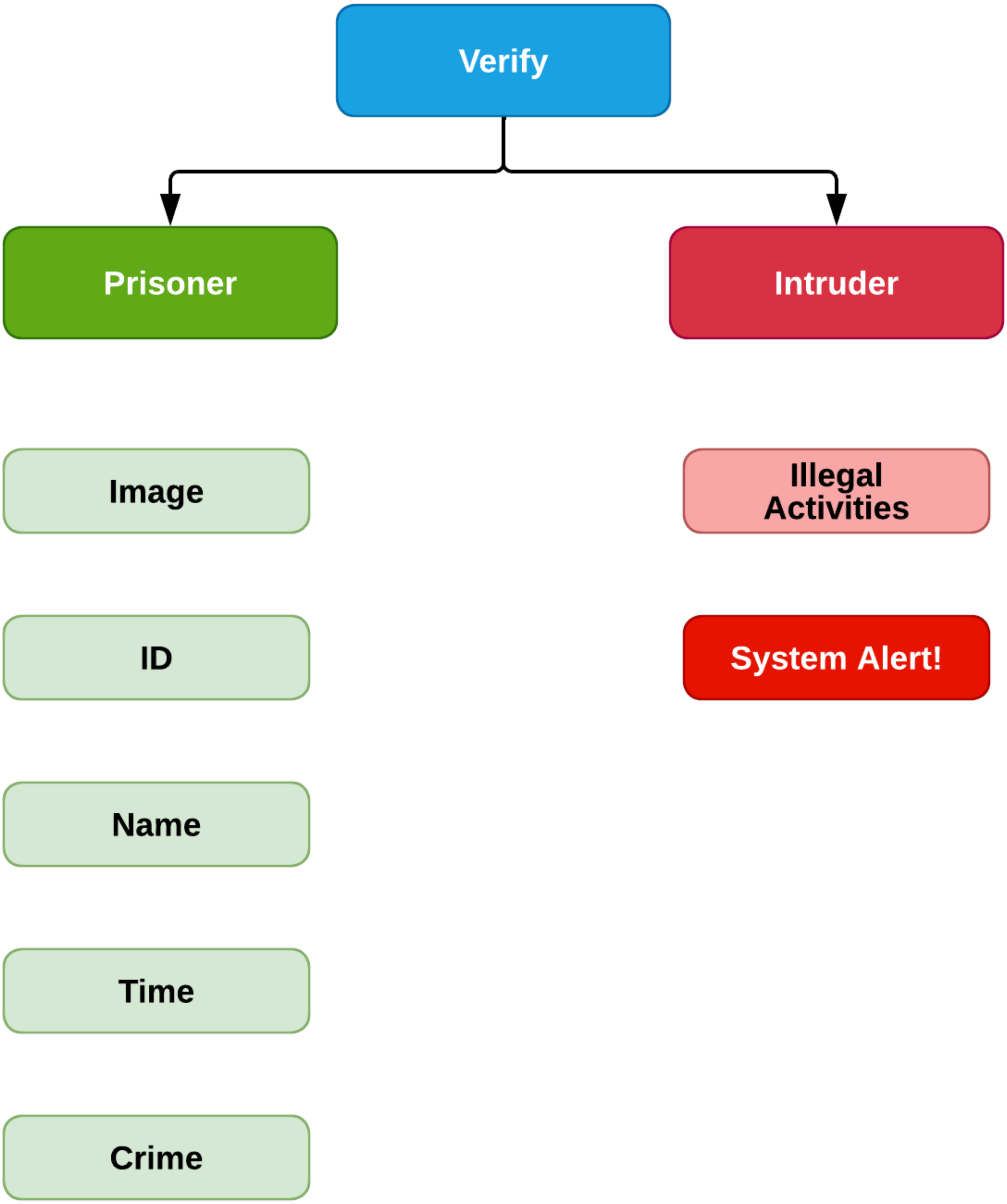
System Architectural Design

The camera will capture an image of anyone inside the prison facilities. Then the camera will process this image with the system. After that, the camera will extract the person’s facial features and put them in a template for future verification.

This data is going to be recorded and saved in the database. If the person’s identity matches the database, then that person will have access approval. If not, then that person will have access denial, which will cause a system alert, and warn the guards.



Input/Output



User Interface Design

a. Audience

System users are the “Administrative / Operation Officers” in prison facilities.

b. Strategy

Our main Strategy:

- Safeguard any prison facility from any danger or illegal activities.
- Create an integrated, easy-to-use interface. So, new employees can be trained to use our platform in a matter of days.
- Report immediately to the security department if any danger occurs.

c. Words

The text used in the system is meaningful and simple to understand for the user, to create a simple communication and interaction between the user and the system, as too much or complex information may overwhelm the user.

d. Visual representations

This concerns graphical elements used in the system like images, interactive buttons, and icons, …. The system has buttons like “Add Personnel”, “Face Recognition”, and “Training”.

e. Physical Objects or space

The user should interact with the system through the prison computers only. The user should be authorized to access the prison system due to data integrity & confidentiality.

f. Time

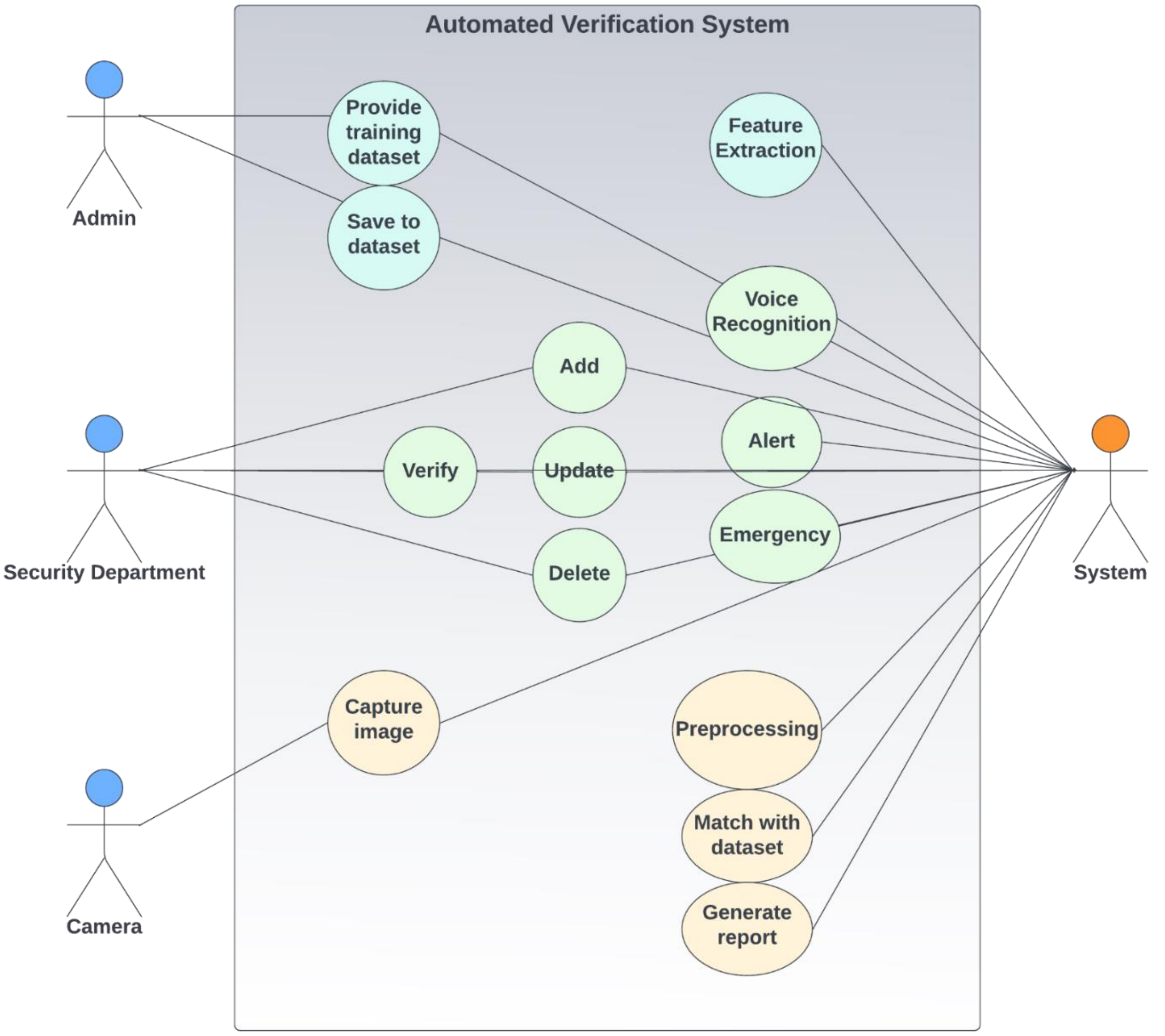
Mostly refers to the media that changes with time such as real-time video streaming. Motion plays a crucial role in the facial recognition process.

g. Behaviour

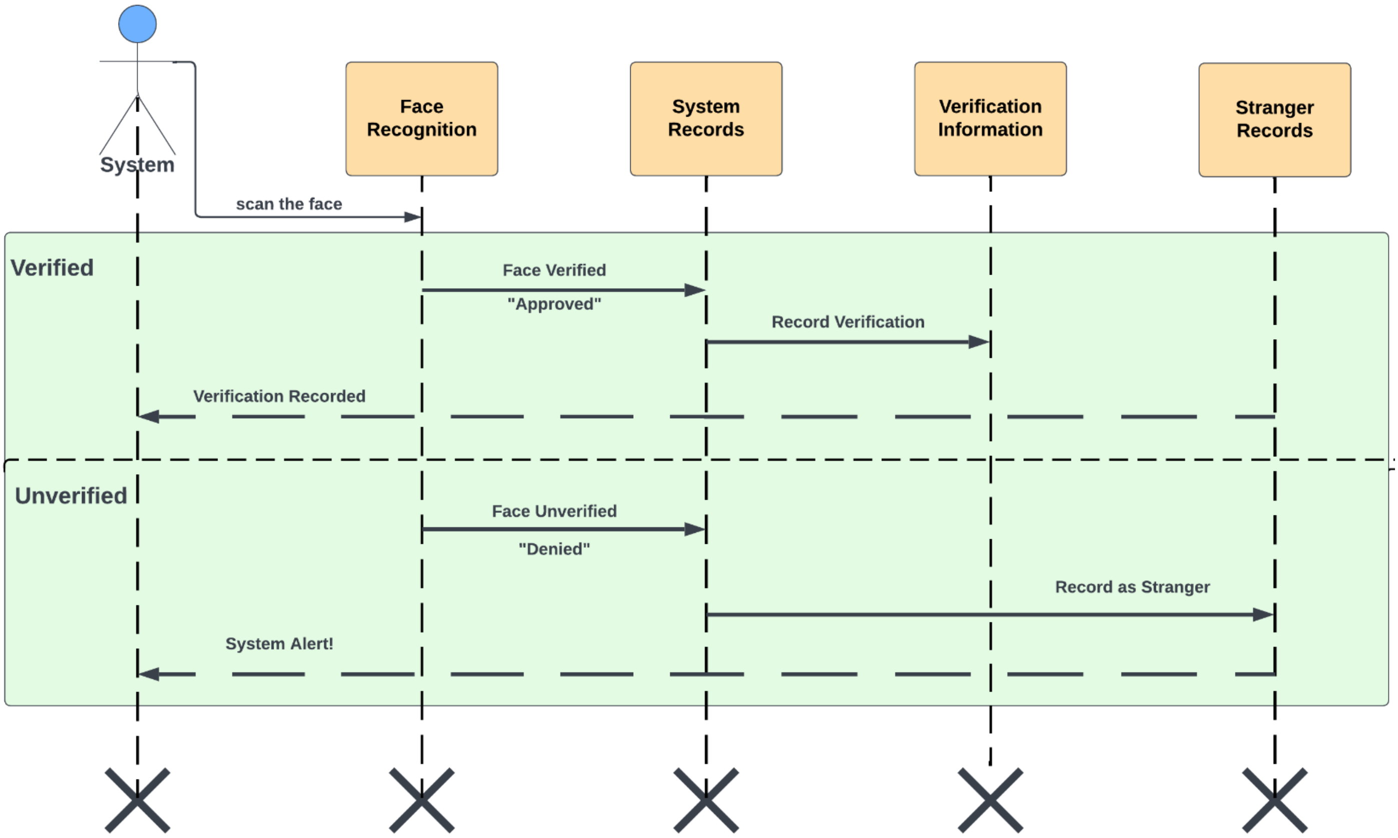
This includes the mechanism of the system: how do users perform actions on the system? How do users operate the system? *[It was explained briefly in the Application Description "System Interface" Section]*

Diagrams

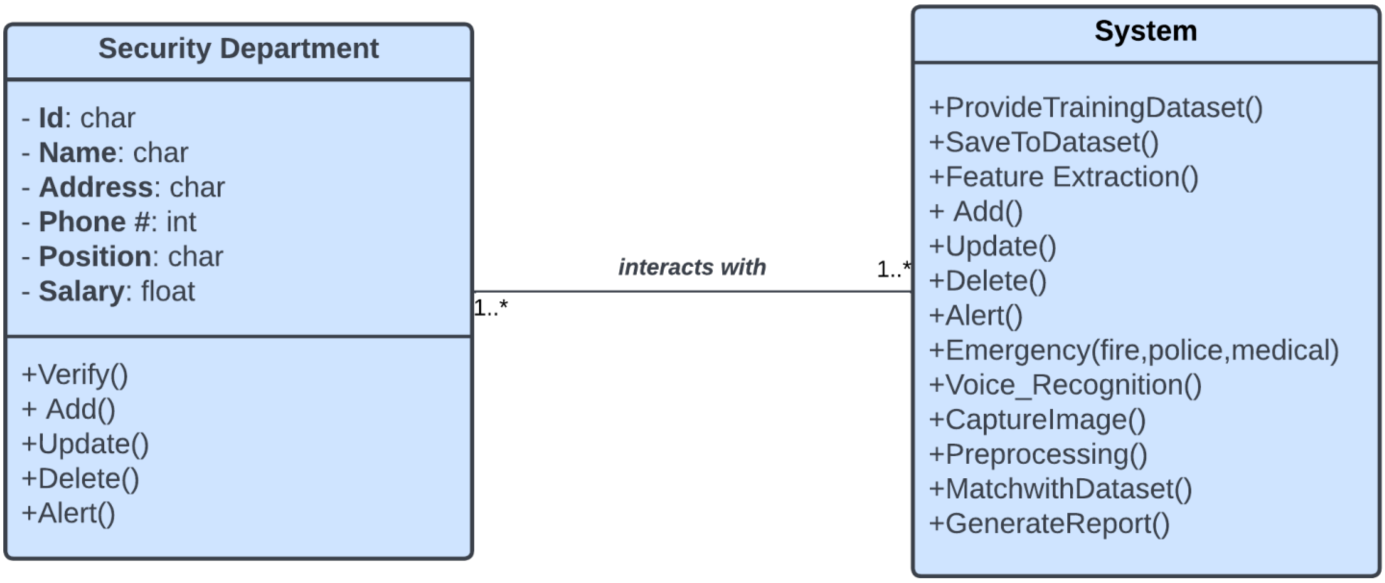
Use Case



Sequence Diagram



Class Diagram



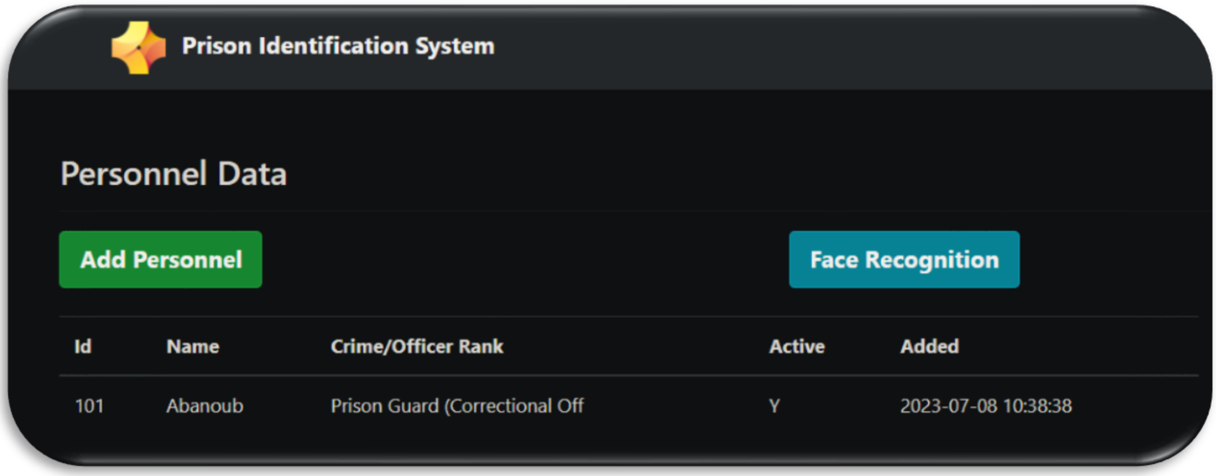
Chapter V: Conclusion & Future Work

In conclusion, facial recognition technology has advanced significantly and has established itself as a trustworthy and effective tool for a variety of applications, including security systems, online authentication, and social media tagging. Face recognition algorithms have improved with machine learning and deep learning, making them more reliable and accurate.

However, the ethical and privacy issues around the usage of this technology, as well as its dependability in various lighting and environmental circumstances, remain issues that must be resolved. Additionally, more complex algorithms that can account for changes in face expressions, ageing, and occlusions must be created.

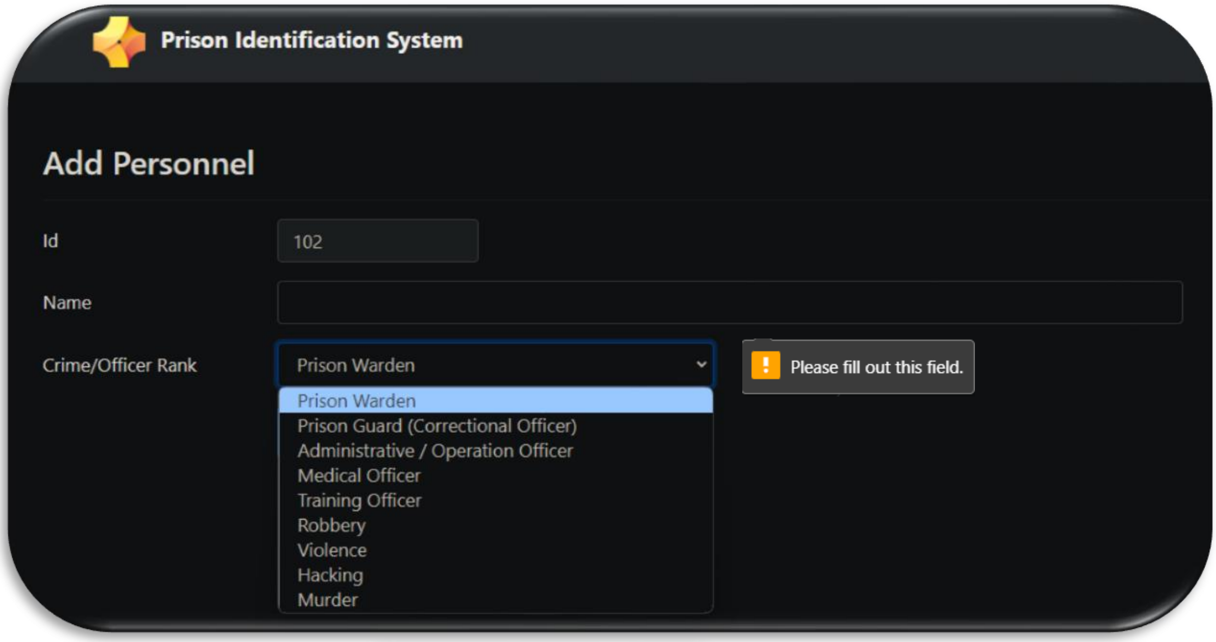
In terms of future work, researchers and engineering need to concentrate on creating facial recognition systems that are safer, more accurate, and more dependable. To make sure that this technology is used ethically and in a way that respects privacy rights, guidelines and laws must also be created. Additionally, more study is required to enhance the performance of face recognition systems under difficult circumstances like dim lighting and occlusions. Last but not least, facial recognition technology may find new uses in a variety of sectors if it is combined with other cutting-edge technologies like augmented reality and virtual reality.

System Screenshots



Personnel Data

Id	Name	Crime/Officer Rank	Active	Added
101	Abanoub	Prison Guard (Correctional Off	Y	2023-07-08 10:38:38


Prison Identification System

Add Personnel

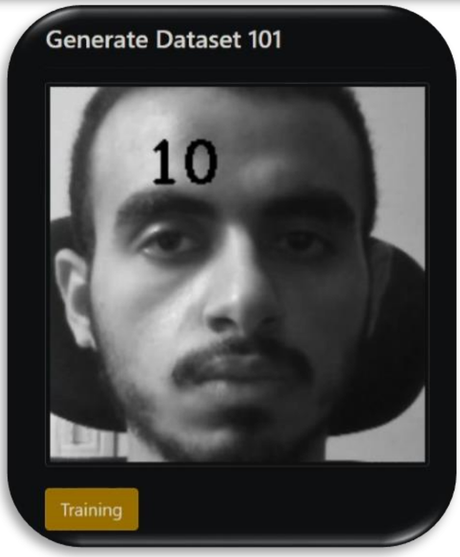
Id: 102

Name:

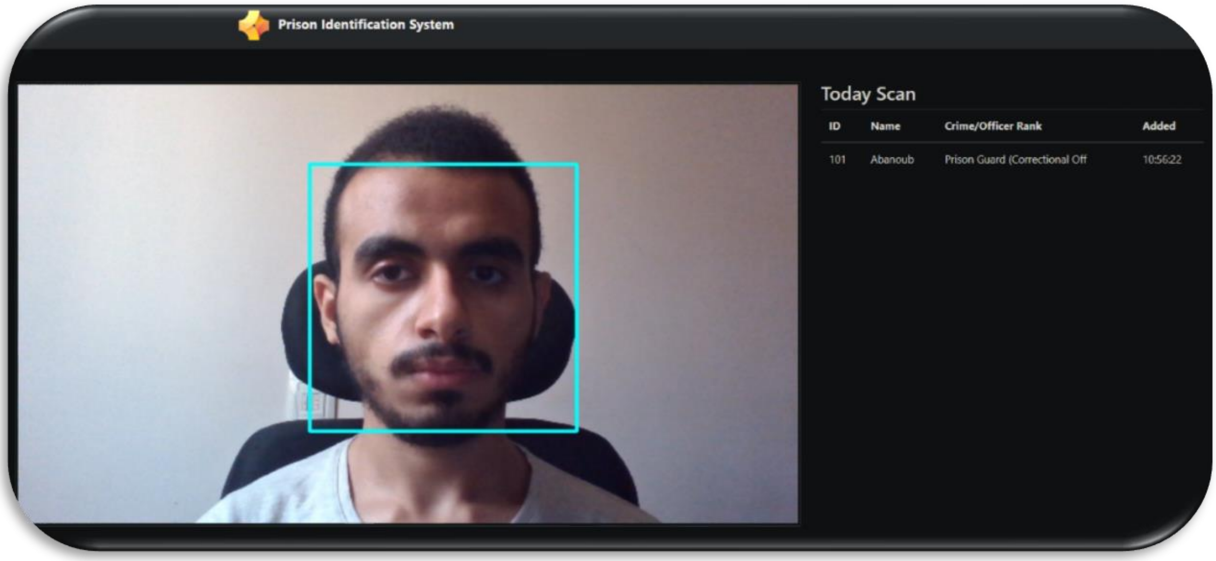
Crime/Officer Rank: Prison Warden

Please fill out this field.

Prison Warden
Prison Guard (Correctional Officer)
Administrative / Operation Officer
Medical Officer
Training Officer
Robbery
Violence
Hacking
Murder

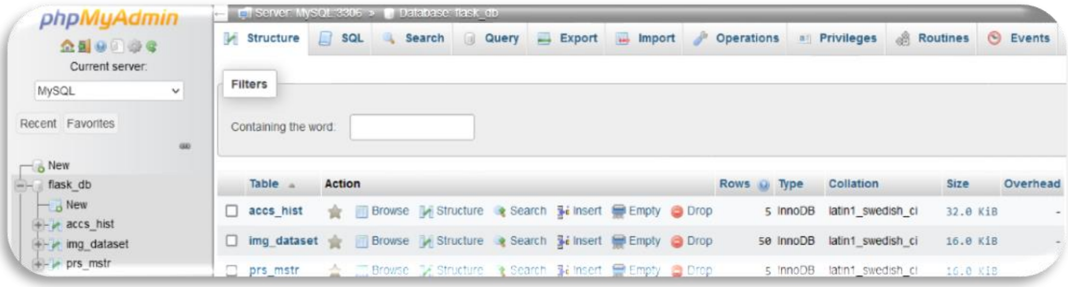


Generate Dataset 101



Today Scan

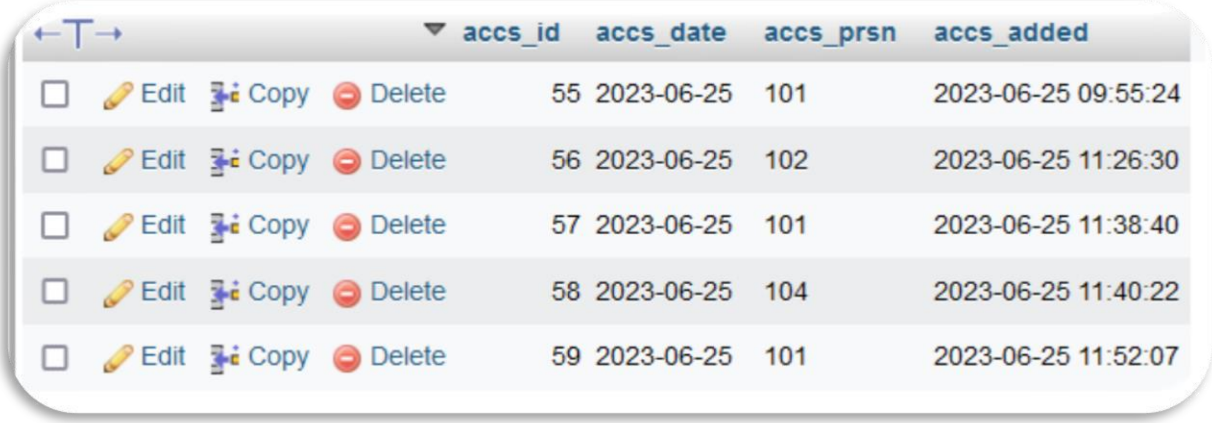
ID	Name	Crime/Officer Rank	Added
101	Abanoub	Prison Guard (Correctional Off	10:56:22



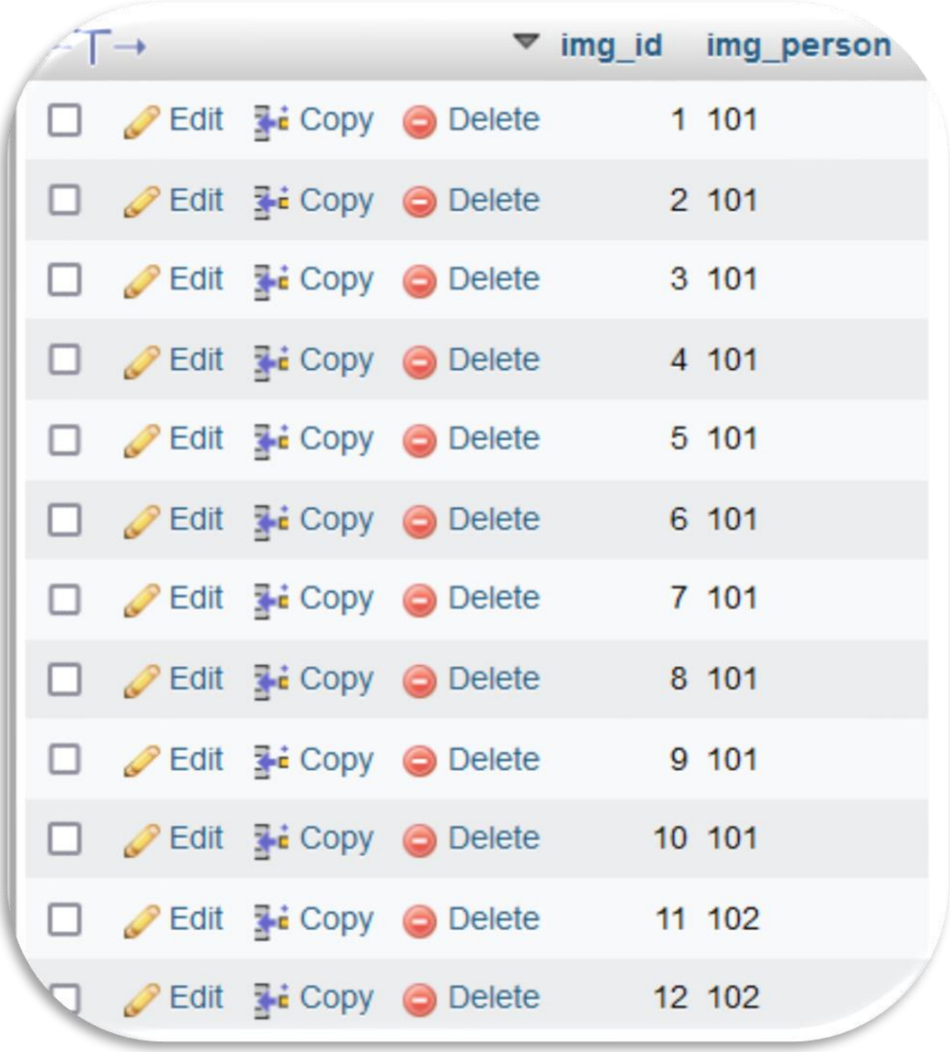
Containing the word:

	Table	Action	Rows	Type	Collation	Size	Overhead
□	accs_hist	Browse Structure Search Insert Empty Drop	5	InnoDB	latin1_swedish_ci	32.0 KiB	-
□	img_dataset	Browse Structure Search Insert Empty Drop	50	InnoDB	latin1_swedish_ci	16.0 KiB	-
□	prs_mstr	Browse Structure Search Insert Empty Drop	5	InnoDB	latin1_swedish_ci	16.0 KiB	

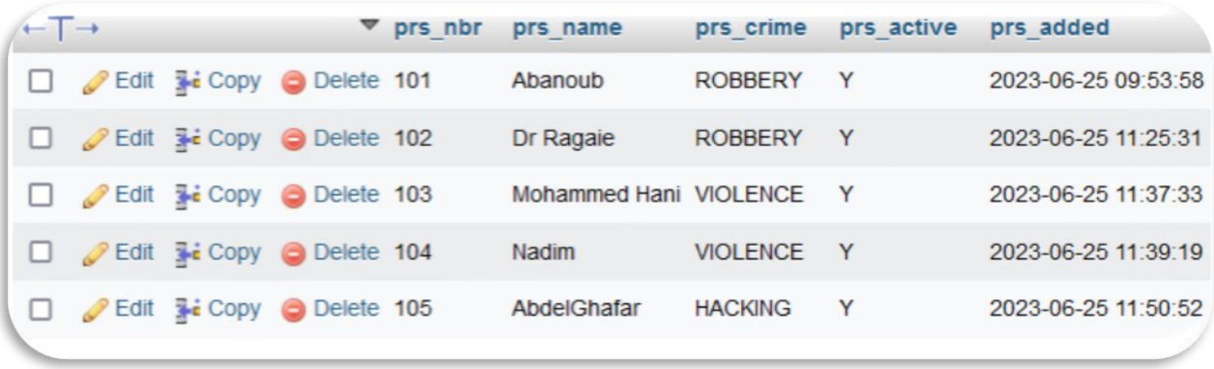
WampServer



←T→				accs_id	accs_date	accs_prsn	accs_added
□	Edit	Copy	Delete	55	2023-06-25	101	2023-06-25 09:55:24
□	Edit	Copy	Delete	56	2023-06-25	102	2023-06-25 11:26:30
□	Edit	Copy	Delete	57	2023-06-25	101	2023-06-25 11:38:40
□	Edit	Copy	Delete	58	2023-06-25	104	2023-06-25 11:40:22
□	Edit	Copy	Delete	59	2023-06-25	101	2023-06-25 11:52:07



←T→				img_id	img_person
□	Edit	Copy	Delete	1	101
□	Edit	Copy	Delete	2	101
□	Edit	Copy	Delete	3	101
□	Edit	Copy	Delete	4	101
□	Edit	Copy	Delete	5	101
□	Edit	Copy	Delete	6	101
□	Edit	Copy	Delete	7	101
□	Edit	Copy	Delete	8	101
□	Edit	Copy	Delete	9	101
□	Edit	Copy	Delete	10	101
□	Edit	Copy	Delete	11	102
□	Edit	Copy	Delete	12	102



←T→				prs_nbr	prs_name	prs_crime	prs_active	prs_added
□	Edit	Copy	Delete	101	Abanoub	ROBBERY	Y	2023-06-25 09:53:58
□	Edit	Copy	Delete	102	Dr Ragaie	ROBBERY	Y	2023-06-25 11:25:31
□	Edit	Copy	Delete	103	Mohammed Hani	VIOLENCE	Y	2023-06-25 11:37:33
□	Edit	Copy	Delete	104	Nadim	VIOLENCE	Y	2023-06-25 11:39:19
□	Edit	Copy	Delete	105	AbdelGhafar	HACKING	Y	2023-06-25 11:50:52

More Information

Images play an important role in today’s information age. A single image represents a thousand words. They are produced at a high rate and can be found everywhere. A reason for all this is because cameras and other photo equipment has become cheap and easily accessible. Today we have image retrieval systems like Google’s image search, where we can easily search for images using keywords. But getting the computer to understand the semantics inside of images isn’t easy. The reason for this is simply because the computer can’t understand the context. In this paper we will talk about a problem that is very complex and common, namely face recognition. Identifying and comparing faces in images is a very complex task, this is probably why it has attracted so many researchers in the latest years. We will also describe some of the problems you will meet when designing a face recognition system, and we will take a closer look on how real-life systems solves these issues. Common methods like feature extraction, holistic matching and hybrid methods will be discussed. We will also take a closer look at a promising approach that uses 3D modelling.

Research on automatic face recognition systems has been conducted now for almost 60 years. The first paper talking about face recognition can be traced back to the 1950s in psychology. The first work concerning automatic face recognition was done in 1970 by Kelly. His thesis describes a computer program which performs a complex image-processing task. The task was to find the same person in a set of images taken by a TV camera. Interest concerning face recognition is spread among different research environments, not only among computer scientists. It all started with psychologists, but over the last 40 years, extensive research has been conducted by psychophysicists, neuroscientists, and various types of engineers.

Psychophysicists and neuroscientists have been concerned with issues such as whether face perception is a dedicated process or not. This issue is still being debated in the psychology community. During the 1980s, work on face recognition had no progress. But the interest grew rapidly again from the beginning of the 1990s. gives some reasons why the research interest increased: real-time hardware became more available, and the importance of surveillance-related applications increased. This paper contains four sections. The first section describes problems designers meet when creating a face recognition system. The second section describes various approaches taken in designing a face recognition system; it also describes some real-life systems. The third section tries to describe the future. The fourth section concludes this paper.

In identifying a face, we usually give an image as input to a face recognition system. The process in recognizing the face is done in three key steps: (1) Face detection, locating the face in the image. (2) Feature/component extraction, a feature/component may be the eyes, the nose or the chins. (3) Recognition, comparing the input image with the ones in the database [9]. The result of this process will hopefully be a set of images that are similar to the input image. The result will be returned to the user of the system. A face recognition system needs to compare its input images to a set of known images. These images are often stored in databases. There are several problems that may occur when comparing a database image with an input image. The main concern is of course that all images of the same face are heterogeneous. When image databases are created they contain good scenario images. These images are often taken in good condition. But this isn’t always the case. Examples of bad scenarios are when the face area is unfocused and too small, this is often the case of input images. A face recognition system needs to solve the problem concerning different facial expressions as well. The system must be able to know that two images of the same person with different facial expressions is the same person. Other issues face recognition systems need to solve is Makeup, posing positions, illumination conditions, and comparing images of the same person with and without glasses.

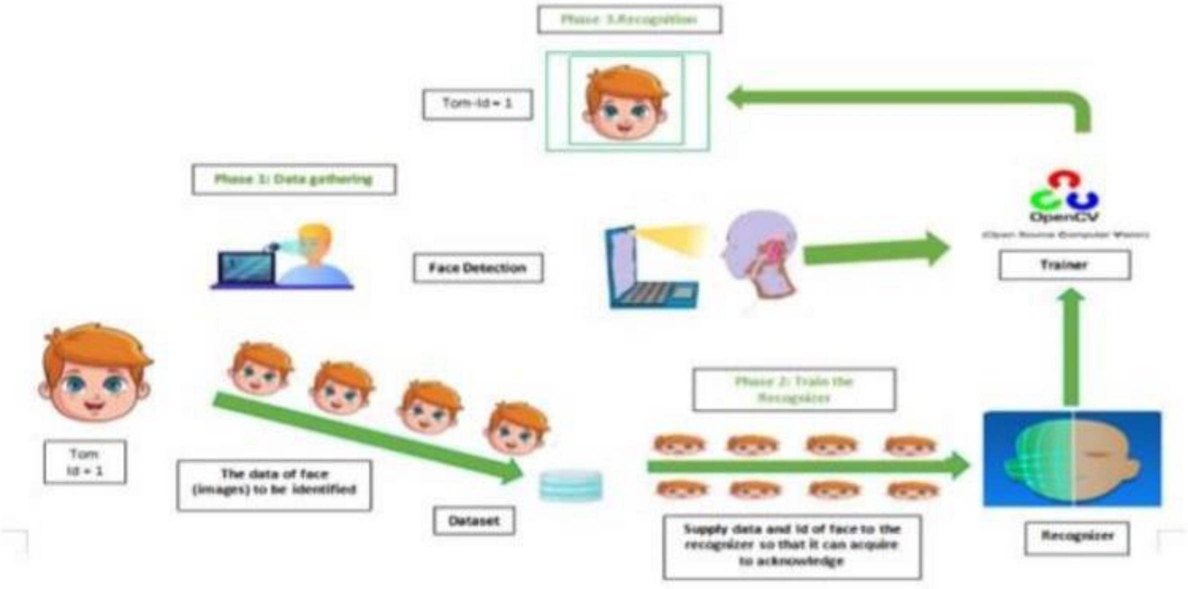
In the beginning of the 1970’s, face recognition was treated as a 2D pattern recognition problem. The distances between important points were used to recognize known faces. E.g., measuring the distance between the eyes or other important points or measuring different angles of facial components. But the main focus has been on making face recognition systems fully automatic.

OpenCV (Open-Source Computer Vision Library) is a library of programming functions mainly aimed at real time computer vision, developed by Intel. It is free for use. The library is cross-platform. It focuses mainly on real-time image processing. The OpenCV Library is a collection of low-overhead, high-performance operations performed on images. The OpenCV implements a wide variety of tools for image interpretation. It is compatible with Intel® Image Processing Library (IPL) that implements low-level operations on digital images. In spite of primitives such as linearization, filtering, image statistics, pyramids, OpenCV is mostly a high-level library implementing algorithms for calibration techniques (Camera Calibration), feature detection (Feature) and tracking (Optical Flow), shape analysis (Geometry, Contour Processing), motion. Analysis (Motion Templates, Estimators), 3D reconstruction (View Morphing), object segmentation and recognition (Histogram, Embedded Hidden Markov Models, Eigen Objects). The essential feature of the library along with functionality and quality is performance. OpenCV has so many capabilities it can seem overwhelming at first. Some of them are as follows:

a) General computer-vision and image-processing algorithms (mid-and low-level APIs).
b) High-level computer-vision modules.
c) AI and machine-learning methods.
d) Image sampling and view transformations.
e) Methods for creating and analysing binary images.
f) Methods for computing 3D information.
g) Math routines for image processing, computer vision, and image interpretation.
h) GUI methods.

The advancement of man-made intelligence is currently in full swing, and it is presenting us with enormous prospective outcomes. With the use of man-made reasoning improvements, investigation, gauging, and detecting were taken to a new level. Computer vision has recently emerged as an extremely promising subject of study. It is the process of recognizing people's faces in photos & videos.

This capability is incredibly powerful, despite enormous variations in visual upgrades due to changing conditions, maturing, and interruptions such beards, glasses, and hairstyle changes. A numerical as well as computational method in face recognition system which speedy and is fast to take attendance. It can recognize the face of an individual with the help of the camera to mark attendance. The purpose is to calculate large amount of data at a time so that it will be speedy and help to reduce the effort and the time. The research will focus on face recognition attendance system bases on OpenCV library.


Phase 3.Recognition
Tom-Id = 1
Phase 1: Data gathering
Face Detection
OpenCV
(Open Source Computer Vision)
Trainer
Tom
Id = 1
The data of face (images) to be identified
Dataset
Phase 2: Train the Recognizer
Supply data and Id of face to the recognizer so that it can acquire to acknowledge
Recognizer

The coronavirus disease (COVID-19) is an unparalleled crisis leading to a huge number of casualties and security problems. In order to reduce the spread of coronavirus, people often wear masks to protect themselves. This makes face recognition a very difficult task since certain parts of the face are hidden. A primary focus of researchers during the ongoing coronavirus pandemic is to come up with suggestions to handle this problem through rapid and efficient solutions. In this paper, we propose a reliable method based on occlusion removal and deep learning-based features in order to address the problem of the masked face recognition process.

The first step is to remove the masked face region. Next, we apply three pre-trained deep Convolutional Neural Networks (CNN), namely VGG-16, AlexNet, and ResNet-50, and use them to extract deep features from the obtained regions (mostly eyes and forehead regions). The Bag-of-features paradigm is then applied to the feature maps of the last convolutional layer in order to quantize them and to get a slight representation compared to the fully connected layer of classical CNN. Finally, Multilayer Perceptron (MLP) is applied for the classification process. Experimental results on Real-World-Masked-Face-Dataset show high recognition performance compared to other state-of-the-art methods.

COVID-19 can be spread through contact and contaminated surfaces; therefore, the classical biometric systems based on passwords or fingerprints are no anymore safe. Face recognition is safer without any need to touch any device.

Recent studies on coronavirus have proven that wearing a face mask by a healthy and infected population reduces considerably the transmission of this virus. However, wearing a mask face causes the following problems: fraudsters and thieves take advantage of the mask, stealing and committing crimes without being identified. Community access control and face authentication have become very difficult tasks when a grand part of the face is hidden by a mask. Existing face recognition methods are not efficient when wearing a mask which cannot provide the whole face image for description. Exposing the nose region is very important in the task of face recognition since it is used for face normalization, pose correction, and face matching. Due to these problems, face masks have significantly challenged existing face recognition methods.

To tackle these problems, we distinguish two different tasks, namely face mask recognition and masked face recognition. The first one checks whether the person is wearing a mask or not. This can be applied in public places where the mask is compulsory. Masked face recognition, on the other hand, aims to recognize a face with a mask based on the eyes and the forehead regions. In this paper, we handle the second task using a deep learning-based method. We use a pre-trained deep learning-based model to extract features from the unmasked face regions (out of the mask region). It is worth stating that the occlusions in our case can occur in only one predictable facial region (nose and mouth regions); this can be a good guide to handling this problem efficiently.

Occlusion is a key limitation of real-world 2D face recognition methods. Generally, it comes out from wearing hats, eyeglasses, masks as well as any other objects that can occlude a part of the face while leaving others unaffected. Thus, wearing a mask is considered the most difficult facial occlusion challenge since it occludes a grand part of the face including the nose. Many approaches have been proposed to handle this problem. We can classify them into three categories, namely the local matching approach, the restoration approach, and the occlusion removal approach. Matching approach: Aims to compare the similarity between images using a matching process.

Generally, the face image is sampled into a number of patches of the same size. Feature extraction is then applied to each patch. Finally, a matching process is applied between probe and gallery faces. The advantage of this approach is that the sampled patches are not overlapped, which avoids the influence of occluded regions on the other informative parts. For example, Martinez and Aleix [20] sampled the face region into a fixed number of local patches. Matching is then applied for similarity measure.

Other methods detect the key points from the face image, instead of local patches. For instance, Weng et al. proposed to recognize persons of interest from their partial faces. To accomplish this task, they firstly detected keypoints and extracted their textural and geometrical features. Next, point set matching is carried out to match the obtained features. Finally, the similarity of the two faces is obtained through the distance between these two aligned feature sets. The keypointbased matching method is introduced in Duan et al. SIFT keypoint descriptor is applied to select the appropriate keypoints.

Gabor ternary pattern and point set matching are then applied to match the local keypoints for partial face recognition. In contrast to the above-mentioned methods based on fixed-size patches matching or keypoints detection, McLaughlin et al. applied the largest matching area at each point of the face image without any sampling. Restoration approach: Here, the occluded regions in the probe faces are restored according to the gallery ones. For instance, Bagchi et al. proposed to restore facial occlusions.

The detection of the occluded regions is carried out by thresholding the depth map values of the 3D image. Then, the restoration is taken on by Principal Component Analysis (PCA). There are also several approaches that rely on the estimation of the occluded parts. Drira et al. applied a statistical shape model to predict and restore the partial facial curves. Iterative closest point (ICP) algorithm has been used to remove occluded regions in . The restoration is applied using a curve,which uses a statistical estimation of the curves to manage the occluded parts. Partially observed curves are completed by using the curves model produced through the PCA technique.

Occlusion removal approach: In order to avoid a bad reconstruction process, these approaches aim to detect regions found to be occluded in the face image and discard them completely from the feature extraction and classification process. Segmentation-based approach is one of the best methods that detect firstly the occluded region part and using only the non-occluded part in the following steps. For instance, Priya and Banu divided the face image into small local patches. Next, to discard the occluded region, they applied the support vector machine classifier to detect them. Finally, a mean-based weight matrix is used on the non-occluded regions for face recognition. Alyuz et al. applied an occlusion removal and restoration. They used the global masked projection to remove the occluded regions.

Next, the partial Gappy PCA is applied for the restoration using eigenvectors. Since the publication of AlexNet architecture in 2012 by Krizhevsky et al., deep CNN has become a common approach in face recognition. It has also been successfully used in face recognition under occlusion variation. It is seen that the deep learning-based method is founded on the fact that the human visual system automatically ignores the occluded regions and only focuses on the non-occluded ones. For example, Song et al. proposed a mask learning technique in order to discard the feature elements of the masked region for the recognition process. Inspired by the high performance of CNN-based methods that have strong robustness to illumination, facial expression, and facial occlusion changes, we propose in this paper an occlusion removal approach and deep CNN-based model to address the problem of masked face recognition during the COVID-19 pandemic. Motivations and more details about the proposed method are presented in the following sections.

Motivated by the efficiency and the facility of the occlusion removal approaches, we apply this strategy to discard the masked regions. Experimental results are carried out on Real-world Masked Face RecognitionDataset (RMFRD) and Simulated Masked Face Recognition Dataset (SMFRD) presented in. We start by localizing the mask region. To do so, we apply a cropping filter in order to obtain only the informative regions of the masked face (i.e., forehead and eyes). Next, we describe the selected regions using a pre-trained deep learning model as a feature extractor. This strategy is more suitable in real-world applications comparing to restoration approaches. Recently, some works have applied supervised learning on the missing region to restore them such as in.

This strategy, however, is a difficult and highly time-consuming process. Despite the recent breakthroughs of deep learning architectures in pattern recognition tasks, they need to estimate millions of parameters in the fully connected layers that require powerful hardwarewith high processing capacity and memory. To address this problem, we present in this paper an efficient quantization-based pooling method for face recognition using three pre-trained models. To do so, we only consider the featuremaps at the last convolutional layers (also called channels) using Bag-of-Features (BoF) paradigm. The basic idea of the classical BoF paradigm is to represent images as orderless sets of local features.

To get these sets, the first step is to extract local features from the training images, each feature represents a region from the image. Next, the whole features are quantized to compute a codebook. Test image features are then assigned to the nearest code in the codebook to be represented by a histogram. In the literature, the BoF paradigm has been largely used for handcrafted feature quantization to accomplish image classification tasks. A comparative study between BoF and deep learning for image classification has been made in Loussaief and Abdelkrim. To take full advantage of the two techniques, in this paper we can consider BoF as a pooling layer in our trainable convolutional layers. This aims to reduce the number of parameters and makes it possible to classify masked face images.

This deep quantization technique presents many advantages. It ensures a lightweight representation that makes the real-world masked face recognition process a feasible task. moreover, the masked regions vary from one face to another, which leads to informative images of different sizes. The proposed deep quantization allows classifying images from different sizes in order to handle this issue. Besides, the Deep BoF approach uses a differentiable quantization scheme that enables simultaneous training of both the quantizer and the rest of the network, instead of using fixed quantizationmerely to minimize the model size. It is worth stating that our proposed method doesn’t need to be trained on the mission region after removing the mask. It instead improves the generalization of the face recognition process in the presence of the mask during the pandemic of coronavirus.

The images of the used dataset are already cropped around the face, so we don’t need a face detection stage to localize the face from each image. However, we need to correct the rotation of the face so that we can remove the masked region efficiently. To do so, we detect 68 facial landmarks using Dlib-ml open-source library introduced in. According to the eye locations, we apply a 2D rotation to make them horizontal as presented in Fig. 2. The next step is to apply a cropping filter in order to extract only the non-masked region. To do so, we first normalize all face images into 240 × 240 pixels. Next, we partition a face into blocks. The principle of this technique is to divide the image into 100 fixed-size square blocks (24 × 24 pixels in our case). Then, we extract only the blocks including the non-masked region (blocks from number 1 to 50). Finally, we eliminate the rest of the blocks as presented in.

From the I th image, we extract feature maps using the feature extraction layer described above. In order to measure the ResNet-50 network architecture introduced in. The extracted DRF are shown the similarity between the extracted feature vectors and the codewords also called term vectors, we applied the RBF kernel as a similarity metric as proposed. Thus, the first sub-layer will be composed of RBF neurons, each neuron is referred to as a codeword. As presented in, the size of the extracted featuremap defines the number of the feature vectors that will be used in the BoF layer.

Here, we refer by Vi to the number of feature vectors extracted from the i t h image. For example, if we have 10 × 10 feature maps from the last convolutional layer of the chosen pre-trained model,wewill have 100 feature vectors to feed the quantization step using the BoF paradigm.

To build the codebook, the initialization of the RBF neurons can be carried out manually or automatically using all the extracted feature vectors overall the dataset. The most used automatic algorithm is of course k-means. Let F the set of all the feature vectors, defined by: F = {Vi j , i = 1 . . . V, j = 1 . . . Vi } and Vk is the number of the RBF neurons centers referred by ck . Note that these RBF centers are learned afterward to get the final codewords. The quantization is then applied to extract the histogram with a predefined number of bins, each bin is referred to a codeword. RBF layer is then used as a similarity measure, it contains 2 sub-layers: RBF layer & Quantization layer.

Once the global histogram is computed, we pass to the classification stage to assign each test image to its identity. To do so, we apply the Multilayer perceptron classifier (MLP) where each face is represented by a term vector. Deep BoF network can be trained using back-propagation and gradient descent. Note that the 10-fold cross-validation strategy is applied in our experiments on the RMFRD dataset. We note V = [v1, . . . , vk] the term vector of each face, where each vi refers to the occurrence of the term i in the given face. T is the number of attributes, and m is the number of classes (face identities). Test faces are defined by their codeword V. MLP uses a set of term occurrences as input values (vi) and associated weights (wi) and a sigmoid function (g) that sums the weights and maps the results to output (y). Note that the number of hidden layers used in our experiments is given by: (m+t)/2 .

The face images were firstly pre-processed as describe. In contrast to SMFRD dataset, RMFRD is imbalanced (5,000 masked faces vs 90,000 non-masked faces). Therefore, we have applied an over-sampling by cropping some non-masked faces to get an equivalent number of cropped and full faces. Next, using the normalized 2D faces, we employ the three pre-trained models (VGG-16, AlexNet and ResNet-50) separately to extract deep features from their last convolutional layers as presented in Sect. 4.2. The output features are (14 × 14 × 512, 13 × 13 × 256, 7 × 7 × 2048) dimensional, respectively. The quantization is then applied to extract the histogram of a number of bins as presented in Sect. 4.3. Finally, MLP is applied to classify faces. In this experiment, the 10-fold cross-validation strategy is used to evaluate the recognition performance. The experiments are repeated ten times in RMFRD and SMFRD datasets separately, where 9 samples are used as the training set and the remaining sample as the testing set, and the average results are calculated.

References

[1] S. Singh, B. Hazela, P. Asthana and A. Pal, “Face Recognition Attendance System,” vol. 11, no. 5, 2023.

[2] M. R. Hasan, R. Guest and F. Deravi, “Presentation-Level Privacy Protection Techniques for Automated Face Recognition,” 2023.

[3] H. Kumar, N. Bhati, P. Bharadwaj, P. Chaudhary and M. Sharma, “Real-Time Face Attendance System Using Face Recognition,” 2023.

[4] M. . K. Rusia and D. K. Singh, “A comprehensive survey on techniques to handle face identity threats: challenges and opportunities,” 2023.

[5] N. Vora and D. Shekhawat, “Comparative Study of Target Image Detection using Deep Learning,” vol. 5, no. 2, 2023.

Links

1. **www.iosrjen.org**
2. **www.easychair.org**
3. **www.junikhyatjournal.in**
4. **www.researchgate.net**
5. **www.springer.com**