order number: .....

Thesis submitted to the

UNIVERSITY OF MOHAMED BOUDIAF – MSILA

FACULTY OF MATHEMATICS AND COMPUTER SCIENCE

DEPARTMENT OF COMPUTER SCIENCE

In partial fulfillment of the requirements for the degree of

Master in Computer science

By:

LATTRAG Nihal

BAGHDADI Aya

Title of the thesis:

Face Recognition Based Access Control Systems

Under the supervision of
Abdessattar Ghemougui

Composition of the jury

Bouguerra Abdelbaki	University of M'sila	President
Ghemougui Abdessettar	University of M'sila	Reporter
Amraoui Noureddine	University of M'sila	Examiner

Acknowledgements

At the end of this modest work, I thank God the Almighty for granting us to have accomplished this work, which presents the fruit of several months of sacrifices. I sincerely thank Mr Ghemouguis promoters for their confidence in our capabilities. I would also like to thank the members of the jury who will do me the honour of judging him and enriching him with their proposals. I would also like to thank everyone who contributed directly or indirectly to this project.

Dedication

It is with genuine gratitude and warm regard that we dedicate this work to our parents and to all our families and friends.

Summary

Abstract

Facial recognition has become a thriving area so that it has been introduced in many areas in all conceptual means of personal telephones and computers in my project, which I have used in the area of accessibility to secure premises So that the person's face is recognized in all the enclosures, this recognition is based on a camera so that the visual information extracted from the captured face is compared with the information stored in the database and the search for access rights. Our system is based on VggFace and we use dlib library and face recognition.

Keywords:Face recognition, Access control, Vggface, dlib, CNN.

Résumé

La reconnaissance faciale est devenue un domaine florissant de sorte qu'elle a été introduite dans de nombreux domaines dans tous les moyens conceptuels de téléphones personnels et d'ordinateurs dans mon projet, que j'ai utilisé dans le domaine de l'accessibilité pour sécuriser les locaux afin que le visage de la personne soit reconnu dans toutes les pièces jointes, cette reconnaissance est basée sur une caméra afin que l'information visuelle extraite du visage capturé soit comparée à l'information stockée dans la base de données et à la recherche de droits d'accès. Notre système est basé sur VggFace et nous utilisons la bibliothèque dlib et la reconnaissance faciale.

Mots-clés: Reconnaissance faciale, Contrôle d'accès, Vggface, dlib, CNN.

Contents

List of Figures

General Introduction

The need to preserve the security of information and material property has become an important focus of many researchers, and has increased attention to it in the past decades to the many challenges they have faced, from cybercrime, fraud, security cards, computer hackers or security violations in companies, banks, residential buildings and other private and public property. In most known crimes, criminals exploit a fundamental flaw in the traditional access control system that depends on our passwords, phone numbers, ID cards, PIN or mother's surname. These means are merely a authentication method. If someone gets this ID, they will be able to access our personal property at any time. In recent times, technology has allowed verification of real individual identity, relying on technology in a field called "biometrics", biometrics are a technology that measures the physiological properties of documentation.

Such as fingerprints, iris, retina, face, sound, etc. Each of these features offers a certain level of accuracy. However, the face retains the ability to recognize a distance of several metres and does not require knowledge or cooperation, so that the demand for it increases to cope with the raging COVID-19 epidemic [23]. Biospatial data-based access control is a highly recommended system for several processes and in several areas to replace traditional systems. This is because it provides a high level of security and improves the reliability of control.

Today, this type of system is made possible by the development of computers and technological means. It depends on converting unique physiological or behavioral properties into a digital version. Identification and validation are then done through a statistical comparison between a digital reference copy and another obtained in real time.

The transition from physiological to digital is mainly about the primitive stage of distinctive extraction. In this study, the "CNNs" method was used. Synthetic neural networks are deep learning algorithms that take input images and wrap them with filters or beads to extract features. The NxN image is assembled with a fXf filter and this casing process learns the same feature on the entire image. The window slides after each operation and features are learned through feature maps. Premium cards capture the local photo reception area and

operate jointly. We used a VGG type of deep CNN method [24].

Our work focuses on the general problem of facial access in the context of video surveillance. Thus,In this brief, we will have to design and implement an app that allows access to recognize people's faces in real time, based on a webcam The system's outputs are to allow entry, transit or interdiction and to report an attempt of inadmissible entry by comparing the characteristics of the faces extracted with the access rights of the base with those found in real time on the camera. We chose to focus our study on three main categories: Chapter I devotes a glimpse of accessibility to biometric profiles and uses.

Chapter II details on facial recognition and methods used before.

Chapter III We talked about the approach to research and steps results.

Finally, the general conclusion will summarize the findings of the various approaches and give some perspectives on future work.

CHAPTER 1

INTRODUCTION TO ACCESS CONTROL SYSTEMS

1.1 Introduction

Access control is one of the most important ways of security. In this chapter, we touched on a definition of it with its purpose and applications in the areas of life and we touched on the most modern methods used at this time, biometric we talked about its division and the date of its appearance.

1.2 Access control systems

An access control system is a security method that is divided into two parts, physical and logical, i.e. specialized equipment and software designed to be organized in one place. The system is designed to restrict, monitor or record and control entry points (doors, gates, checkpoints, etc). The system translates the operation into a request, which is then forwarded to a reference monitor that controls access to the resource. If the subject is allowed to access the object according to the applicable security policy, then access to the object is granted and the process can continue normally. Most of the basic ideas surrounding this story were developed in the early 1970s. An access control matrix, which describes a subject's rights to system resources, is a structure with one row per subject and one column per object in the system. The cells at the intersection of rows and columns describe the subject's access rights to the object [25].

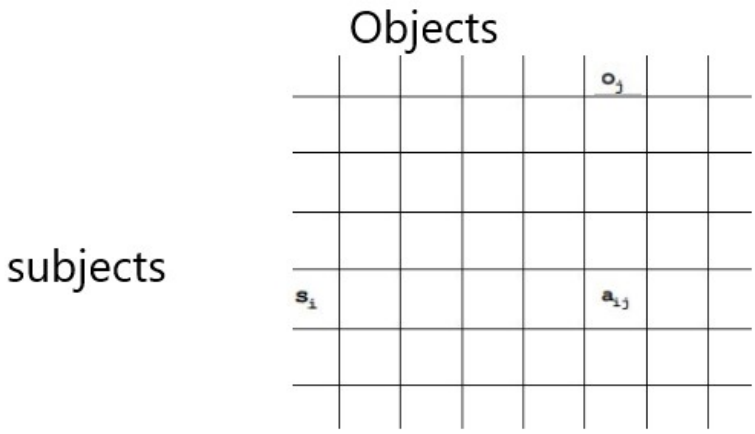

Figure 1.1: subject and object[1]

The above matrix shows the si object with access rights i, j for the object oj. The access control matrix-based model does not provide any specific interpretation of the subjects, objects, or access rights, but they are usually the original entities of the system, and the accuracy of the subject and object definitions depends on the system. Some common definitions are subject user, process, device, object file, relationship in a database, or variable in a program. The following figure shows the basic model for all access control policies [25].

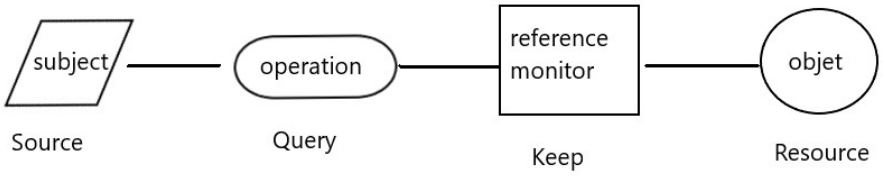

Figure 1.2: The basic model of access control [1]

1.2.1 Applications

The primary goal of an access control system is to restrict access to a specific resource (area, material, or information) to a well-defined set of individuals for a well-defined period o time, and to track authorized or denied access requests. Access control grants entities faces to the requested resource, whether physical (access to buildings, rooms, vaults, etc.) or logical (access to specific folders, programs, information, etc.) [26]. Access control systems has applications in many areas:

1.2.1.1 Computers and phones

1. Use phone accessibility to allow a person to log in to a phone as well as the laptop. They can also be used to store private information.

2. Use them in bilateral authentication on media sites such as Facebook and Instagram.

1.2.1.2 For any organization in any field of activity

1. Restricted access to office space;

2. control the movement of employees within the building;

3. Automatic attendance recording;

1.2.1.3 Healthcare (Hospitals, Pharmacies, Sanatoria)

1. Restricted access to office space, including the storage of certain medications;
2. Fingerprint-based drug procurement control;

1.2.1.4 Power structures (Prisons, Colonies, Places of pre-trial detention)

1. Location and movement of staff and prisoners;
2. Notice of attempted entry into the service building;
3. Restrict access to information and archives;

1.2.1.5 Financial institutions (Banks, Instant payment systems)

1. Biometric ATM;
2. Biometric bank, postal and warehouse units;

1.2.1.6 Educational Iistitutions (Schools, Universities, Libraries)

1. Restricted access to educational institutions;
2. Notify parents of arrival and departure from educational institutions;

1.2.1.7 Railway stations, Airports, Bus fleets

1. Restricted access to offices and departments (for example, only registered passengers);
2. Identify permanent passengers through facial recognition; luggage check such as face recognition;

1.2.2 Type of access control systems

The literature distinguishes three types of access control, administrative, physical and logical.

1.2.2.1 Administrative control

Administrative control primarily involves employees. The human factor is a company's biggest security risk. Therefore, it is necessary to develop appropriate security policies and use administrative controls. The principle of administrative control is to strengthen the security system without the use of technology, mainly checking everything related to human resources [26].

1.2.2.2 Physical control

Physical access controls are particularly infringing on the premises of facilities and equipment. Preventing unauthorized personnel from accessing sensitive areas and even preventing employees from modifying their work equipment is a company security focus. The principle of physical control is to use any method that can prevent, monitor, or prevent unprivileged entities from having physical access to the system to be protected. Surveillance cameras are widely used to track access to commercial areas, security guards, armored doors, security locks and even biometrics [26].

1.2.2.3 Logic control

Companies are becoming more and more dependent on IT and networks. Therefore, they need to apply security policies to the company's network and computer systems with appropriate logical access controls. Logical access control uses processes to restrict the actions of accounts on logical systems/networks [26].

1.2.3 Access control management steps

1.2.3.1 Identification

A person requesting permission to access a resource must first identify themselves in the system. It shows who you are. The identification phase does not prove that you are who you say you are. This means that we can define ourselves as managers, even though we are really just employees [26].

1.2.3.2 Authentication

Verification means that the subject's identity is established by any method, selective or imposed. This process takes place immediately after identification. Several methods can be used: Proprietary biometric means (facial fingerprint, fingerprint, voice, retina scan, etc.) [26].

1.2.3.3 Access Rights

The access requester was granted permission or their request was denied. If so, only the applicant is granted access. Otherwise, they will be informed that the application has been refused, usually for specific reasons[26].

1.2.3.4 Traceability

All actions are tracked and stored in the database. This data will be very useful in a potential audit[26].

1.2.4 Access control models

Access control models are usually involved with whether or not subjects, or any entity that may method data (i.e. a user, a user method, or a system process), have access to the objects, and therefore the entities through that data flows through the actions of the topic (i.e., a directory and a file monitor, keyboard, memory, storage, printer) and the way this access would possibly occur. Access control models ar usually seen as frameworks for implementing and guaranteeing the integrity of security policies that outline however data is accessed and shared on a system. the foremost in style, oldest, and most well-known access control models ar necessary to access control and discretionary access control, however the inherent limitations of each have stirred any analysis into alternatives together with role-based access control, dynamic written access control, and domain sort social control [27].

1.2.4.1 Mandatory access control (MAC)

Loosely outlined as any access control model that enforces security policies freelance of user operations, necessary Access control is typically related to the 1973 BellLaPadula Model[of multi-level security[27].

1.2.4.2 Discretionary access control (DAC)

MAC, whereas vastly vital to military applications, isn't the foremost wide used methodology of access control. That distinction belongs to DAC mostly because of spawning from primarily industrial and educational analysis similarly because the integration of DAC Access control integration into UNIX system, FreeBSD, and Windows 2000. DAC was developed to implement Access control Matrices outlined by Lampson in his paper on system protection. Access control Matrices area unit sometimes pictured as three-dimensional matrices wherever rows area unit subjects, columns area unit objects and also the mapping of subject and object pairs leads to the set of rights the topic has over the object [27].

1.2.4.3 Role-based access control(RBAC)

RBAC is taken into account a way additional generalized model than either mackintosh or DAC, encompassing each models as special cases whereas providing a policy-neutral framework that permits RBAC to be bespoken on a per-application basis. As a mix of the mackintosh and DAC models and integri, RBAC is part supported on principles made public in Biba [27].

1.2.4.4 Domain type enforcement(DTE)

Domain type enforcement (DTE) is an extension of type enforcement (TE) and is itself extended into Dynamic typewritten Access control (DTAC). The principle of type enforcement | social control is additional that versatile policy expressions area unit doable once objects area unit appointed to varieties and therefore columns within the access control matrix area unit replaced by varieties.The DTE extension to the present is to assign subjects to domains and complete the matrix transformation that the access control matrix is currently a website definition table (DDT) with rows of domains and columns of varieties. DTAC expanded upon this to incorporate RBAC type administrative controls. it's claimed that DTE models will implement the BellLaPadula confidentiality model moreover as a number of the additional sturdy integrity options in DAC and RBAC. As of yet, this can be not demonstratable [27].

1.3 Biometric systems

The term biometrics is made up of two words - Bio (Greek for life) and Metric (measurements). Biometrics is a branch of information technology that aims to create an individual's identity based on personal traits. Biometrics is currently a buzzword in the field of information security because it provides a high degree of accuracy in identifying an individual [28]. We display biometrics ratings. They are divided into two categories illustrated in Figure1.3, physical and behavioral. The physical part includes physical features such as the face, fingers, hands, retina, and DNA, while the ability features are unique features such as passwords, signature, and voice.

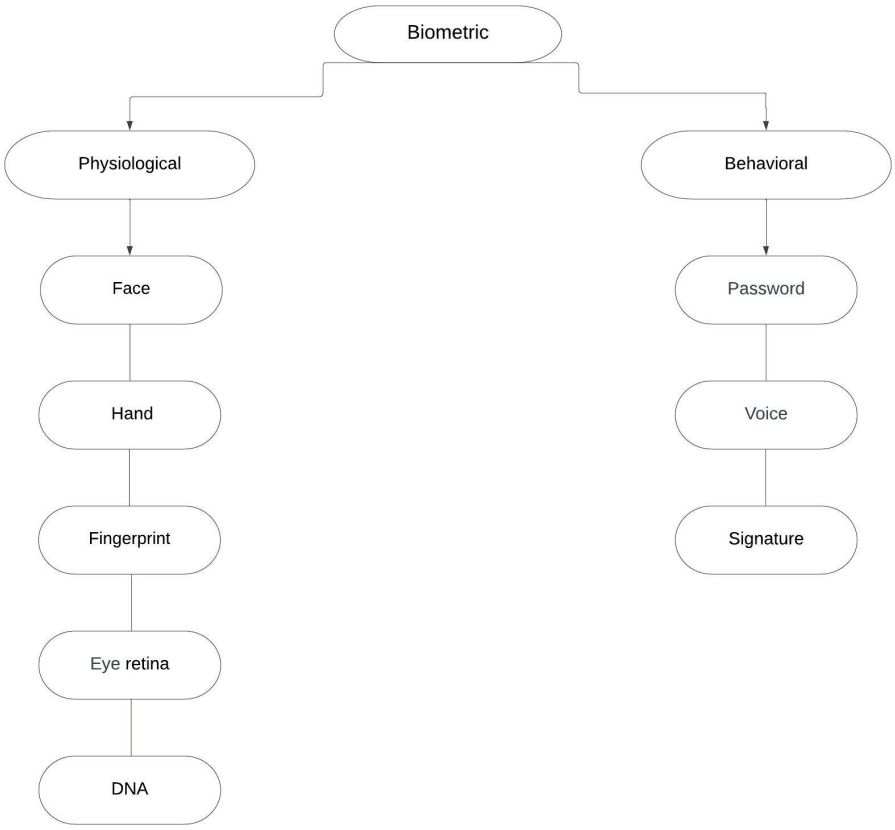

Figure 1.3: Biometric

Since each person has unique features, biometric-based security systems are recommended in environments that need a high level of security. Biometrics is said to be the most secure technology because features such as face, fingers, and voice cannot be borrowed or stolen. While applying biomedical technology, at the same time we will be able to know if a person is using two or more identities [29].

1.3.1 History of biometrics

For years, people have been using physical features such as facial features, voice or the way we walk to identify people. Alphonse Bertillon, who previously headed the police forensics unit in Paris, believes it should be possible to measure different parts of the body, among other features, to identify criminals. Bertillon's idea pioneered a more precise and unambiguous way to identify people based on fingerprints. The idea revolutionized police work and set off a trend among major law firms, all of whom were keen to take part in the discovery. Facilitating police work by storing fingerprints in a database that can later be compared and matched to specific crime scenes [30].

1.3.2 Species are known in biometrics

1.3.2.1 Fingerprint

Since then, fingerprints are one in every one of the main ways to spot someone because of the extent of accuracy. The fingerprint determination and formation happens at a fetal stage within the primary seven months and is measured because of the pattern of ridges and valleys on the fingertip. Recognition by fingerprint is reliable since a person's fingerprints are unique for each finger, even identical twins have different fingerprints [30].

Figure 1.4: Fingerprints[2]

1.3.2.2 Face

Another common biometric system is the recognition by face expression, where an individual is identified through a video or photograph. The recognition is done by measuring the individual's facial characteristics such as the facial shape, placement of the eyes, brows, nose, lips and even the chin. Although there might occur some problems regarding the identification if the person were to e.g wear a covering of the face or heavy makeup if the lighting is different [30].

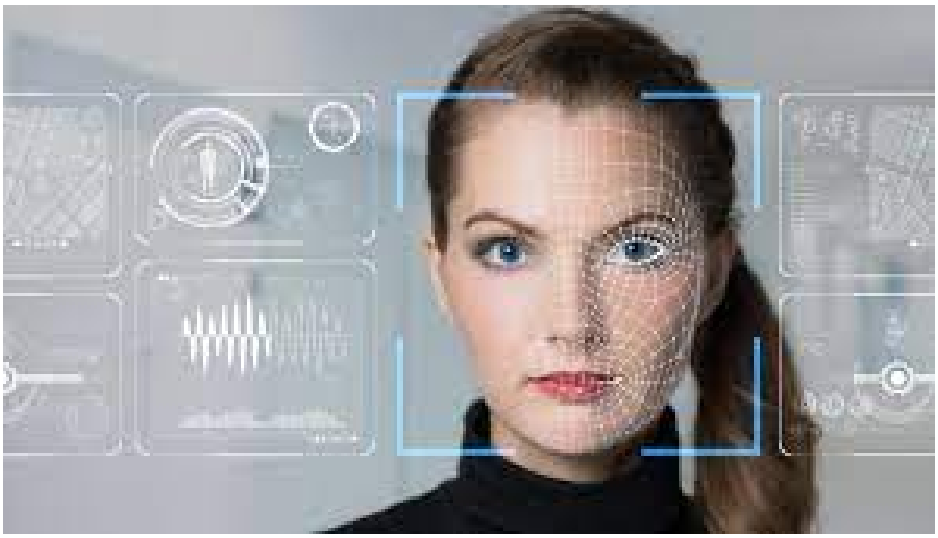

Figure 1.5: Face recognition[3]

1.3.2.3 Iris

Another biometric system is the identification of the eyes which determines the iris. The iris is the coloured ring surrounding the pupil. rather like the fingerprints the iris forms during the fetal stages and stabilizes within the primary two years after being born, the iris varies even on identical twins. The iris carries distinctive information which is tough to temper even after surgery and a synthetic iris is straightforward to detect. For a highly reliable person identification, the system looks at the feel pattern within the iris with numerous individual attributes, e.g stripes, pits and furrows[30].

Figure 1.6: Iris [4]

1.3.2.4 Voice

Lastly among the most biometric systems is voice recognition, it's the way to spot an individual by voice and is split into behavioural and physiological features. Physiological features contain the measurement of shape and size concerning the lips that modifies the voice, vocal tracts and mouth. The behavioural features are determined by the movement of the individual's mouth, jaws and tongue among others as they speak. However, these components can vary over time because of ageing, and emotion yet as changes within the voice e.g when sick. Therefore the voice and its spectral content are analysed to see information regarding the pitch, duration and quality of the voice. There are two ways of doing a voice recognition [30] :

1. Text-dependent, which implies that the system relies on the pronouncement still because of the uttering of a predefined phrase or word.

2. Text-independent, in which the system will recognize the person without the predefined phrase or word. this method is much more complex and is harder to control but it's also very sensitive and also speech recognition is going to suffer from background noise.

Figure 1.7: voice recognition [5]

1.3.3 Other biometrics

Besides these four primary biometric recognition there are more ways of doing a private recognition. as an example [30]:

1. Deoxyribonucleic acid (DNA) includes a structure and pattern that's unique for every human aside from identical twins. it's effective as a biometric identifier since it represents the core of each cell within the body.

2. The ear recognition relies on the structure of the pinna, which is distinctive for each individual. the recognition and identification are done by measuring the space of the salient points of the pinna.

3. A palm print is analogous to a fingerprint. It matches the palm of the human which also contains a pattern of ridges and valleys.

4. A signature may be a way for an individual to put in writing their name which needs a commentary instrument and energy of the signature. This has been accepted as a technique of verification in government, legal and commercial transactions.

1.3.4 Spoofing

Even biometric systems is attacked. Biometric spoofing may be a method that's wont to fool a biometric system. These attacks are different from regular IT attacks.These attacks, there are mostly used with physical tools, like face masks, gummy fingers, printed iris pictures, printed pictures of a face, etc, which might make a biometric system vulnerable and insecure. For a

face recognition system, an image of a real user is held ahead of the camera, which is that the most used attack for this recognition system since it's easy and cheap to induce an image of an individual. It will be taken of the individual that is unaware of it, on the web, etc. There are two other ways in which may be accustomed fool the system furthermore, which are video and 3D models of the real user. Spoofing attacks can happen at different levels of the biometric system [30]:

1. Sensor level attack: The attacker uses a fake biometric characteristic of a real user.
2. Replay attack: The attacker copies the biometric sample and reuses it on the biometric sensor.
3. Trojan Horse attack: A program that makes the required feature set and replaces the feature extractor with it.
4. Spoofing the features: The feature vectors are replaced with fake features.
5. Attack on matcher: employing a computer program attack to vary the match score.
6. Attack on template: Changing the stored templates or substituting them with a replacement one.
7. Attack on communication: To intercept the info within the communication channel and reuse a modified version of the info within the system.
8. Attack on decision module: employing a bug program to alter the ultimate result.

1.3.5 Anti-spoofing

There are different techniques which will be accustomed prevent these attacks which is cited as anti-spoofing [30] :

1. Sensor-Level techniques are supported to use of hardware devices to stop attacks. as an example, a sensor that may detect facial thermogram, pressure, fingerprint sweat, reflection properties of the eyes, etc.

2. Feature-Level techniques is more called a software based technique. it'll detect the spoofing when the information has been obtained and isn't detected directly on the material body as in sensor-level.

3. Score-Level techniques could be a lesser used technique which is created as a further measure to the sensor and feature-Level techniques thanks to its ability to perform. It focuses on understanding the biometric systems at a score-level to boost the protection against attack.

1.4 Conclusion

In this chapter we introduced access control systems, we namly fouced on biometric ones. In the next chapter, we are going to focus on facial detection and recognition.

CHAPTER 2

INTRODUCTION TO FACE DETECTION AND RECOGNITION

2.1 Introduction

Face is one of the most used bio-metrics for authenticating human identity. in the chapter we introduce facial identification, well-known methods, and then we mentioned identification, types and known algorithms, and we touched on deep learning and its uses in facial recognition.

2.2 Face detection

Face detection is an AI-based architecture that will be able to extract and identify human faces from digital images. When integrated with biometric security systems (particularly, identity verification ones), this type of technology is what makes it possible to observe and track people in real-time. In applications that use facial tracking, analysis, and recognition, face detection typically works because of the start. It encompasses a significant impact on how sequential operations within the app will perform. And in face analysis, FD helps identify which parts of an image or video should be focused on to determine age, gender and emotions using facial expressions [31].

2.2.1 Face detection methods

2.2.1.1 Knowledge-based

Knowledge-based methods rely on rule sets and recognize faces based on human knowledge. For example, measure the relative positions of various key elements such as the mouth, nose, and eyes [32], which are then used to classify "face" and "non-face". The problem with this procedure is that it is difficult to clearly define the face. If the definition is too detailed, some faces will be missed, and if the description is too general, the false positive rate will skyrocket [33]. This method alone is not enough to find many faces in multiple images [32].

2.2.1.2 Feature-based

Feature-based methods locate faces by extracting their structural features. It is first trained as a classifier and then used to distinguish between face and non-face regions. The idea is to push the limits of our instinctual knowledge of faces. This multi-step approach, even photos containing multiple faces, has reported a success rate of 94% [33]. These methods use elements that are independent of changes in lighting, orientation, or expression, such as B. texture or skin tone signatures for detection [32].

2.2.1.3 Template matching

Template matching methods use predefined or parameterized face templates to locate or recognize faces through the correlation between the template and the input image. Example: A human face can be divided into eyes, facial contours, nose and mouth [33]. Create feature models of the entire face or parts of the face (mouth, eyes, nose). Then, localization is based on the correlation of these models with candidates [32].It is also possible to create face models from edges using only edge detection methods. This method is easy to implement, but not suitable for face recognition. However, deformable templates have been proposed to deal with these issues [32].

2.2.1.4 Appearance-based

The appearance-based method depends on a group of delegate training face images to search out out face models. it's better than other ways of performance. These methods use the identical principle as presented in the previous point. this method depends on techniques from statistical analysis and machine learning to seek out the relevant characteristics of face images. also utilized in feature extraction for face recognition [33]. The methods belonging to the present category have shown good results compared to the opposite three kinds of methods [32].

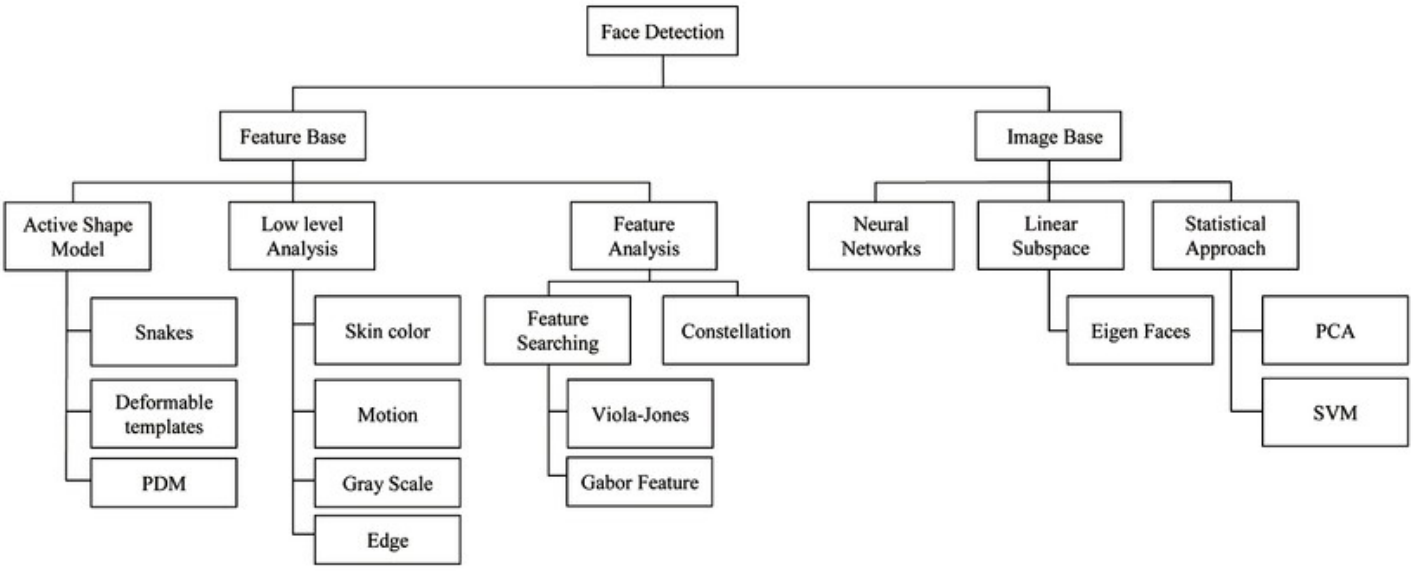

Figure 2.1: Face detection method [6]

2.2.2 Face detection techniques and algorithm

2.2.2.1 Geometric methods for face detection

In the early days of computer vision, researchers studied a number of algorithms that extract image features and use geometric requirements to understand the transfer of all features. This is partly due to very limited computing resources. Reducing information by extracting features made computer vision possible in the first computers [34].

2.2.2.2 Template-based face detection

Most facial recognition algorithms are model-based, and they encode images of faces directly from pixel intensities. Probabilistic models also characterize these images of faces primarily through neural networks or some other mechanism. The parameters of these models are adjusted automatically or manually with example images [34].

2.2.2.3 Simple templates

Most face detection algorithms are model-based, they encode facial images directly on the basis of pixel intensity. Probabilistic models are mostly used for the characterization of these images of facial images also by neural networks or by some other mechanisms. the parameters of these models are automatically adjusted by sample images or manually [34].

2.2.3 How face detection works

Facial detection algorithms usually start by looking for the human eye one of the easiest features to detect. The algorithm can then try to identify the eyebrows, mouth, nose, nostrils and iris. Once the algorithm concludes that it has found a face region, it applies additional tests to confirm that it did indeed detect a face. To ensure accuracy, algorithms must be trained on large datasets containing hundreds of thousands of positive and negative images. The training improves the algorithm's ability to determine whether and where a face is present in the image [31].

2.3 Face recognition

Face recognition is an area in computer vision that is used to identify and identify human faces in images or videos. It is commonly used in many commercial products, such as Facebook,

which uses facial recognition to automatically tag people in photos. Master-card uses facial recognition as a payment method, which they call Selfie Pay. Facial recognition is also being used to automatically capture school attendance. Also used to access secure premises of large corporations when a company registers a host. There are two distinct components of facial recognition: discovery and recognition. Discovery is finding and finding faces in images, while recognition is the task of performing face recognition in images of specific people[35].

2.3.1 Evolution of facial recognition

Following Bledsoe's work, some advances appeared within the following years which improved the accuracy of the results. a number of the new approaches were supported the employment of facial markers on specific areas of the face like the corners of the mouth, eyes or nose, assuming that the outline of their spatial position modded relevant and powerful biometric patterns. Nevertheless, the approaches supported anthropometric techniques didn't achieve the expected results, thus for a few years the research on face recognition techniques failed to like much development. Probably the foremost important turning point came in 2001 when Paul Viola and Michael Jones proposed a framework for object detection that achieved success rates never seen before. Their algorithm was supported the mixture of the utilization of fast computing features (HAAR features) with an optimised training process. during this way it had been possible to detect the face quickly and reliably, and to isolate areas of the image so as to use more powerful descriptors. In recent years the foremost relevant advances within the field of face recognition are made by the utilization of deep learning environments. Unlike classical methods (where the descriptors to be applied on the input image had to be chosen beforehand), deep learning algorithms through the training process create their own feature extractors by analysing complex relationships between the computer file set. the numerous boost in computational power along with the immense amount of images available through the net has allowed deep learning-based automatic face recognition systems to realize very high success rates even within the most demanding environments [36].

2.3.2 Facial recognition applications

Facial recognition is of great interest in many areas including law enforcement and surveillance (video surveillance, access control, and identification of criminals through search warrants).Smart Cards Clash (national identity and passport) Information security (data manage-

ment and file encryption) Entertainment (video games and virtual reality) It can also be used in the healthcare sector (monitoring patients to see if images of other patients have the same symptoms).In this white paper we will discuss access control [37].

2.3.3 Basic steps in facial recognition

The methods used in a facial recognition system vary depending on the application and manufacturer in terms of the methods used, but generally they involve a series of steps that work to capture, process, analyze and match the face with a recorded database of different images; The system captures 80 nodal points on the human face that are used to measure a person's face variables, such as the length and width of the nose, eye depth, and the shape of facial bones in general; Facial recognition steps include [38]:

Detection The facial recognition system is attached to the video monitoring system, it scans the camera's field of view to find out the faces and when any head is detected, it sends to the system to process it, then the system estimates the position, direction and size of the head, but the face must be rotated at least 35 degrees towards the camera so you can discover it.

Normalization The image of the captured face is scaled and rotated so that it can be recorded and mapped to a suitable shape and size and determines the key factors of the face, which include distance between eyes, thickness of lips, distance between chin and forehead and many more, generating what is called a facial signature.

Representation: The system converts the signature into a unique code to facilitate the mathematical comparison of the data with the data recorded in the database.

Matching It is the final stage in which it compares the extracted face data with the previously stored data and returns the facial details matching an image in the database and informs the user of the final result.

2.3.4 Face recognition techniques

In the early 1970s, biometric identification was treated as a controversy of two-dimensional pattern recognition.But it's essential that automatic face recognition systems be fully automatic. Face recognition is such a challenging but interesting problem that attracted researchers with

different backgrounds: psychology, pattern recognition, neural networks, computer vision, and computer graphics [39]. There are three categories of face recognition methods: Holistic Matching Methods,Feature-based (structural) Methods and Hybrid Methods.

2.3.4.1 Holistic matching methods

Holistic face recognition uses global information from faces to perform face recognition [40]. These methods use the entire face area as raw input to the recognition system [41]. To extract features without taking into account their distinct points (eg eye centres, nostrils, mouth centre, etc.). Its main advantages are that it is relatively quick to implement. On the other hand, this method is sensitive on the one hand to differences in lighting, posture, and facial expressions [42]. Global information from faces is mainly represented by a small number of features, which are directly derived from the pixel information of facial images. These small numbers of features capture the contrast between different individual faces and are thus used to uniquely identify individuals. Each face image is represented as a high-dimensional vector signal by the sequence of gray values of all pixels in the face [40]. There are four categorizations of holistic methods that are as follows:

1. Principal Component Analysis (PCA).
2. Linear Discriminant Analysis(LDA).
3. Independent Component Analysis(ICA).
4. Support Vector Machine(SVM).

2.3.4.2 Feature-based (Structural) methods

Feature-based (structural) matching methods. Local features such as eyes, nose, and mouth are first extracted and their location and local statistics (geometry and/or appearance) are fed into a structure classifier. In this method [**?**], the basic principle is to build a local feature space and use appropriate image filters to make the face distribution less affected by various changes. The main advantage of this approach is that differences in position, lighting, and expression can be more easily modeled compared to global approaches [42].There are four categorizations of Feature-based Methods that are as follows [41]:

1. Pure Geometry Methods(PGM).

2. Dynamic Link Architecture(DLA).

3. Hidden Markov Model(HMM).

4. Convolution Neural Networks(CNN).

2.3.4.3 Hybrid methods

Hybrid Methods; Combining the advantages of global and local methods, as the human cognition system uses, by combining the discovery of geometric (or structural) features and the extraction of local appearance features, one could argue that these methods can offer the best of the two types of methods. Increased stability of recognition performance during changes in pose, lighting, and facial expressions [**?**, 42]. There are three methods that areas [41]:

1. Hybrid LFA.

2. Shape Normalized Methods(SNM).

3. Component Based Methods(CBM).

2.4 Face recognition algorithms

2.4.1 Iterative closest point-pased alignment

The goal of the alignment method is to iteratively transform the point cloud by determining translation and rotation parameters based on the next iteration point. When the two point clouds are aligned, the cloud mean squared error becomes the smallest. Therefore, by translating and rotating one of the point clouds relative to the others, the distance between the point clouds is reduced to a minimum. Additionally, the distance to each point in the initial point cloud is determined every second, and the average of all distances is calculated. An important disadvantage of the iterative closest point-based alignment method is that it requires an initial alignment of the convergent history. This method is computationally intensive and therefore has another disadvantage[34].

2.4.2 Simulated annealing-based alignment

It is an algorithm based on a stochastic process used for local research. the difference between hill-climbing and simulated annealing is that it can compute an excellent worse solution than

the present one within the iteration process. As a simulated solution. Six parameters are required for simulated annealing (in which three for each translation also the rotation referencing to a 3D coordinate system) which is employed to define transformation matrix which is employed for an alignment between two 3D faces. this approach aligns images of the face in three phases [34]:

1. alignment in initial level.
2. alignment at an approximate level.
3. alignment within the last level.

Initially, the centre of the two-sided mass is aligned. By using this approach, it serves to attenuate an approximation measure which uses the consensus of multiple estimators M (MSAC) along with the mean square error corresponding point of two faces that may compare. then, an accurate alignment is obtained with the mean of a look algorithm that's based upon simulated annealing, which uses the measurement of the interpenetration of surfaces (SIM) as an estimation criterion. the disadvantage of alignment supported simulated annealing is its more calculation time which is comparable to the alignment based on the nearest iterative point[34].

2.4.3 Average-Butres based face model

this alignment is based on the medium-based face model. First of all, the reference points are on the face automatically or manually. Subsequently, the common of pivotal coordinates calculated, followed by procrustes examination and transformed milestone, are again mediated to get a face model. While during this method, the image of the probe face aligns with the common model using an alignment on the nearest iterative point. A notable weakness of the alignment based on the medium face model is that the low precision index and a part of the spatial material lost during the creation of the medium face model [34].

2.5 Deep learning based face recognition methods

2.5.1 Deep learning

Deep learning is a type of artificial intelligence derived from machine learning where the machine is able to learn through itself-even, unlike the programming where it is content to execute to the letter of predetermined rules. deep learning methods use a cascade of multiple layers of

processing units for feature extraction and transformation. They learn multiple levels of representations that correspond to different levels of abstraction, the amount form a hierarchy of concepts, showing strong in variance to the facial pose, lighting, and expression changes, as shown in Fig 2.2. In 2014, DeepFace and DeepID achieved state-of-the-art accuracy on the famous LFW benchmark, surpassing human performance within the unconstrained scenario for the primary time [7].

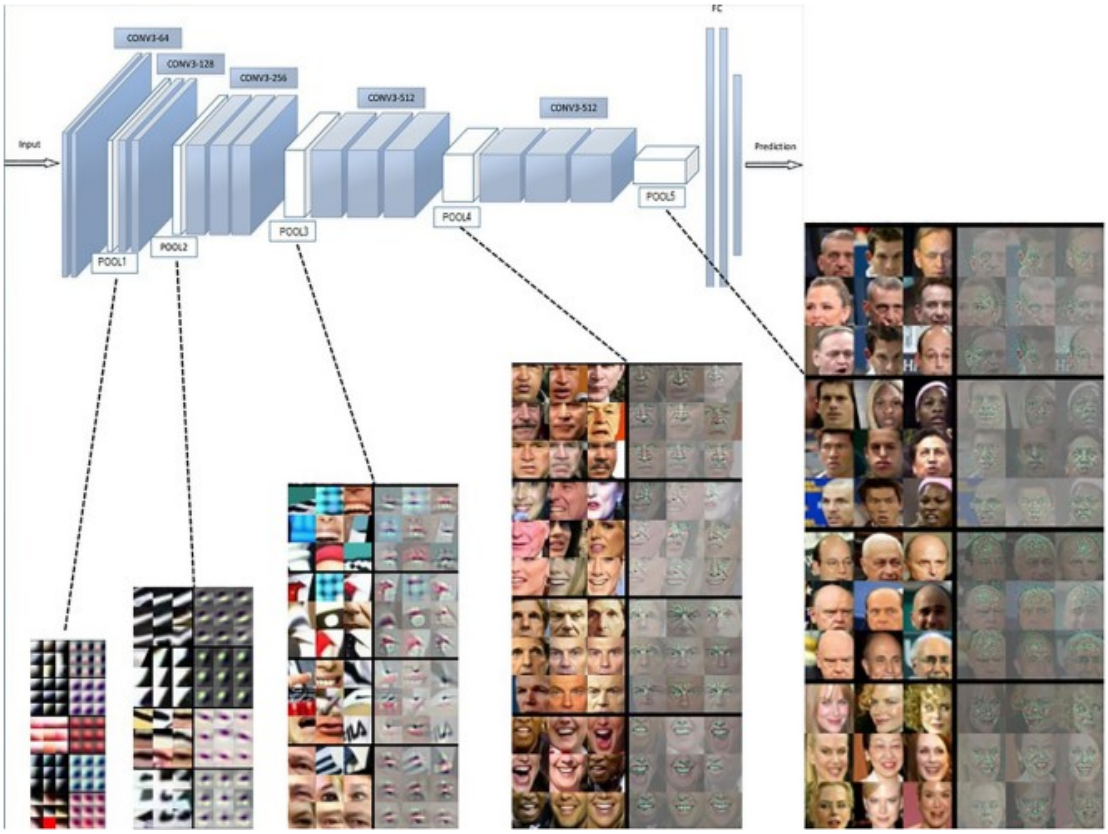

Figure 2.2: Multiple layers of processing units for feature extraction and transformation[7]

2.5.2 Convolutional neural network

A convolutional neural network may be a feed-forward network with the power to extract topological properties from the input image. It extracts features from the raw image and so a classifier classifies extracted features. CNN's are in variance to distortions and easy geometric transformations like translation, scaling, rotation and squeezing. Convolutional Neural Networks combine three architectural ideas to confirm some extent of shift, scale, and distortion in variance: local receptive fields, shared weights, and spatial or temporal sub-sampling. The network is typically trained as a typical neural network by back propagation [43].

2.5.3 Deep learning face recognition models

2.5.3.1 DeepFace

Based on deep convolutional neural networks, DeepFace could be a deep learning face recognition system. Created by Facebook, it detects and determines the identity of an individual's face through digital images, reportedly with an accuracy of 97.35% [44].

2.5.3.2 DeepID

First coined by Yi Sun in his paper deep learning face representation from predicting 10,000 classes, deep hidden identity for generic object detection, counted among the primary models of deep learning for identity verification. DeepID achieved more accuracy than humans on a project [44].

2.5.3.3 VGGFace

Recently, deep learning convolutional neural networks have surpassed classical methods and are achieving state-of-the-art results on standard face recognition datasets. One example of a state-of-the-art model is that the VGGFace and VGGFace2 model developed by researchers at the Visual Geometry Group at Oxford. Although the model may be challenging to implement and resource intensive to coach, it may be easily employed in standard deep learning libraries like Keras through the employment of freely available pre-trained models and third-party open source libraries [44]. The VGGFace refers to a series of models developed for face recognition and demonstrated on benchmark computer vision datasets by members of the Visual Geometry Group (VGG) at the University of Oxford. There are two main VGG models for face recognition at the time of writing; they're VGGFace and VGGFace2 [45].

2.5.3.4 FaceNet

Achieving the state-of-the-art results on standard data sets, FaceNet uses a triplet loss function to be told score vectors for better leads to feature extraction and, thus, biometric authentication.

2.6 Challenges in face recognition

2.6.1 Aging

One of the reasons for changes in facial appearance can be the aging of the human face, which may affect the entire face recognition process[46]; It is another challenge in the facial recognition system [47]. If the time between each photo shoot is large, big changes will occur in a person. According to various studies conducted by scientists, there will be significant changes in an individual's face every 10 years [46]. The effect of aging can be observed under three main unique characteristics [48]:

1. Aging is uncontrollable: it cannot progress or be delayed and is slow and irreversible.
2. Personal signs of aging: Everyone goes through different patterns of aging. These depend on his genes and many other factors, such as health, food, region and weather conditions.
3. Signs of aging depend on time: a person's face at a certain age affects all older faces, but is not affected at a younger age.

Figure 2.3: Aging Challenge [8, 9, 10]

2.6.2 Expressions

The face is one of the most important biometrics as its unique features play an important role in providing human identity and emotions. Different situations cause different moods that result in different emotions and ultimately a change in facial expressions. Different expressions of the same individual are another important factor to be taken into consideration. Human expressions are especially large expressions such as happiness, sadness, anger, disgust, fear and surprise. Micro-expressions are what show rapid facial patterns and occur involuntarily. Macro and partial expressions find their place on a person's face due to changes in one's emotional state and in the wake of these feelings effective identification become difficult [47]. These facial changes can be computed with the help of dense optical flow [46]. The face is one of the most important biological features, as its unique features play an important role in providing human identity and emotion. Different situations lead to different emotions, which in turn lead to different emotions, which ultimately lead to changes in facial expressions. Different expressions of the same person are another important factor to consider. Human expressions are particularly large expressions such as happiness, sadness, anger, disgust, fear, and surprise. Micro-expressions exhibit rapid facial patterns and occur involuntarily. Macro and local expressions find their place on a person's face due to changes in an emotional state, and as these emotions change, effective identification becomes difficult [47]. These facial changes can be computed using dense optical flow [46].

Figure 2.4: Expression [11]

2.6.3 Partial occlusion

Occlusions are objects that hinder algorithms for successfully extracting facial features. They are of two types: Internal are some of the intrinsic biological elements of the face such as the moustache, beard, and even hair. and external are all the items worn by a person that obscure certain features of the face [49]. Such as sunglasses, scarfs, hands, veils, niqab and masks, etc[47].They are generally called partial occlusions. Partial occlusion corresponds to an occluded object. Facial occlusion of less than 50% is considered partial occlusion. Face recognition methods with partial occlusion are classified into three categories [48]:

1. Part-based methods.
2. Feature-based methods.
3. Fractal-Based Methods.

The presence of such components makes the subject diverse and thus makes automatic face recognition difficult [46]. Local methods are used to deal with the problem of partially obscured faces that divide faces into different parts. Another approach that can be applied for this purpose is the near holistic approach in which occlude features, traits and characters are

eradicated and the rest of the face is used as valuable information. Different techniques are being developed by the researchers to cope with this problem [48].

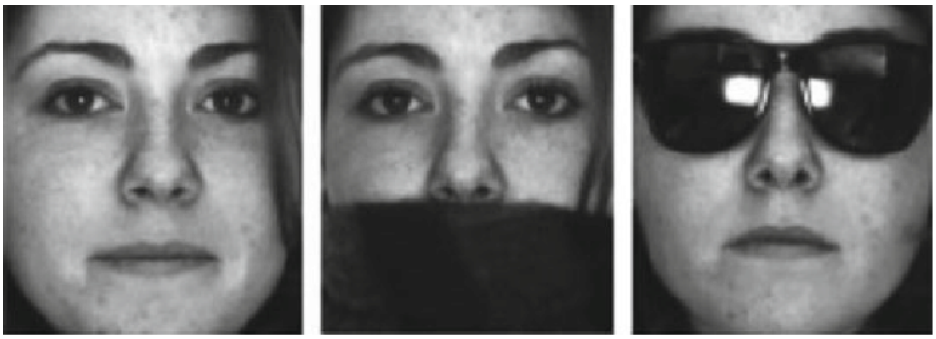

Figure 2.5: Partial Occlusion [12]

2.6.4 Pose in Variance

Variation in pose causes significant problems in detecting a face. For face recognition systems deployed in wild environments like airports, and cities, more reliable algorithms are required. People pose differently every time they take an image. there's no standardized rule for taking a pose. Therefore, it makes harder to differentiate and recognize the faces from images with varying poses. Pose variations degrade the performance of the face expression. additionally, many systems work under inflexible imaging conditions and as a result it affects the standard of gallery images. The methods managing variation in pose are often divided into two kinds i.e. multi-view face recognition and face recognition across pose. Multi-view face recognition is considered as an annexure of frontal face recognition during which gallery image of each pose is considered. On the opposite hand, across a pose in face recognition, yield face with a pose which has never been exposed before to a recognition system [46].

2.6.5 Illuminations

Illumination variation is another factor that not only limits the performance of the face recognition process but the performance of the matching process. for instance, traditional feature-based face detectors, tend to fail under severe illumination variations like heavy shadows and overexposure. like background type, illumination variation are often limited in controlled environments. The angle between the light source, and also the face can generate shadows that mask face features. The matter in question will diminish the flexibility of an algorithm to form an honest identification decision. Moreover, even images from the identical subject can have

large differences. one in all the causes of those differences may be because of the variation of illumination conditions [49].

Figure 2.6: Variation in pose and illumination in face [13]

2.6.6 Similar faces

This is usually a not so common challenge, but we have seen that even humans find it difficult to identify people with similar faces. Hence we can imagine the difficult situation for computer to identify similar face individuals. Especially identical twins with similar facial features, shape etc. this becomes a difficult task for the face recognition system to identify the individual. This will cause an increase in false recognition rate (FRR) as well [46].

Figure 2.7: Similar Faces [14, 15]

2.6.7 Image resolution

The minimum resolution for any standard photo must be 16 * 16. a photograph with a resolution but 16 * 16 is termed a low-resolution photo. These low-resolution images are often found by small standalone cameras like street CCTV cameras, ATM cameras, and supermarket security cameras. These cameras can capture a small a part of the human face area, and since the camera isn't very near the face, it can only capture the face area but 16 * 16. Such an occasional resolution image doesn't provide much information as most of it's lost. It may be quite an challenge within the face recognition process [47].

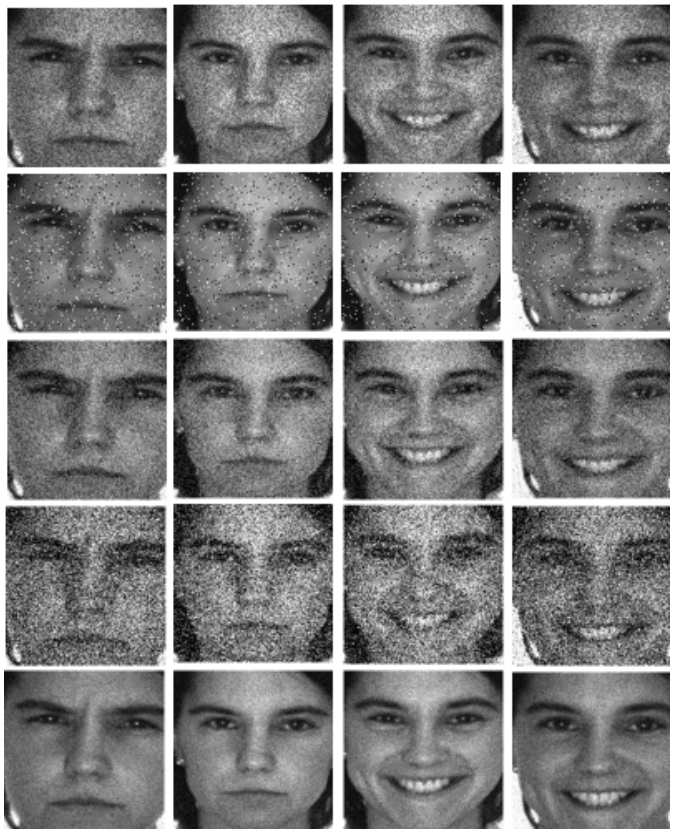

Figure 2.8: Image Resolution [16]

2.6.8 Cosmetic surgery

Esthetical factors can even affect the face recognition identification process. Procedures like cosmetic surgery aim to correct or restore the looks or functionality of visible parts of the anatomy, including the face. Therefore, the markers, and also the templates used for the face recognition process are going to be also impacted. These changes can occur thanks to accidents or regular cosmetic surgery procedures. On the opposite hand, cosmetic surgery may be misused to hide someone's identity with the intent to commit fraud or evade enforcement. Face recognition after cosmetic surgery can cause rejection of genuine users or acceptance of impostors. There are other esthetical factors like bruising or blows that may temporarily change the structure of the markers within the face [49]. Facial beautification is in a position to significantly change the form and texture of the face that's, it affects the utilization of identity verification systems in security applications It also has three sections, which are mentioned within the figure below [50]:

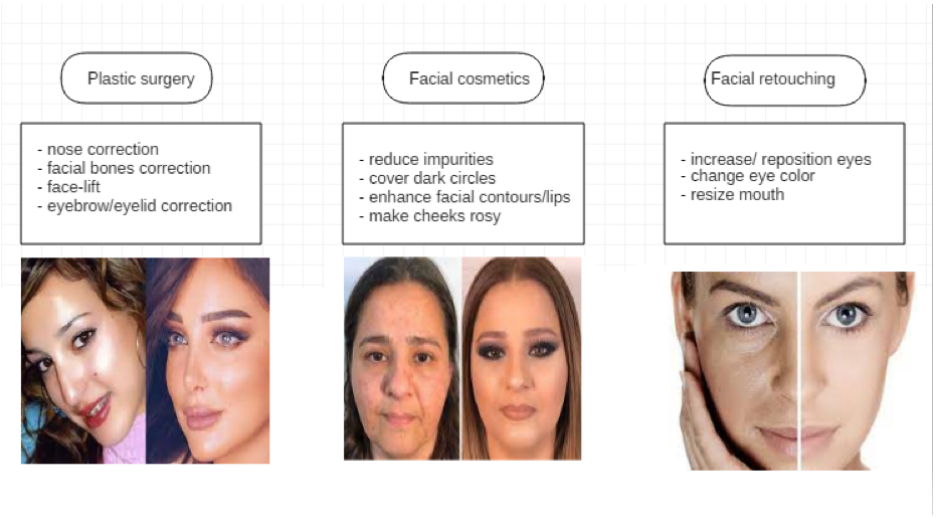

Figure 2.9: Esthetical [17, 18, 19]

2.7 Conclusion

In this chapter, we introduced face recognition, in the next chapter, we will design and implement a face recognition based access control system.

CHAPTER 3

DESIGN AND IMPLEMENTATION OF A FACE RECOGNITION BASED ACCESS CONTROL SYSTEM

3.1 Introduction

This chapter covers the design and implementation of a face recognition based access control system

3.2 System overview

This system propose a facial recognition based solution that helps facilitate contact-less access control. A general overview of the main steps involved in our system is outlined in Figure 3.1. our access control process starts with capturing a digital image of the person to be identified. Then, face detection step is needed to extract the face region from the input image. Next, the extracted face is processed to extract the face recognition data. Then, the authentication process queries the database to check the person's identity and access rights. If the person's facial data matches the data in the database with the appropriate rights, the the person is granted access. However, if the facial data does not match any existing record in the database or, the identified person does not has the access rights, the the access is denied and and an unauthorized access attempt is recorded.

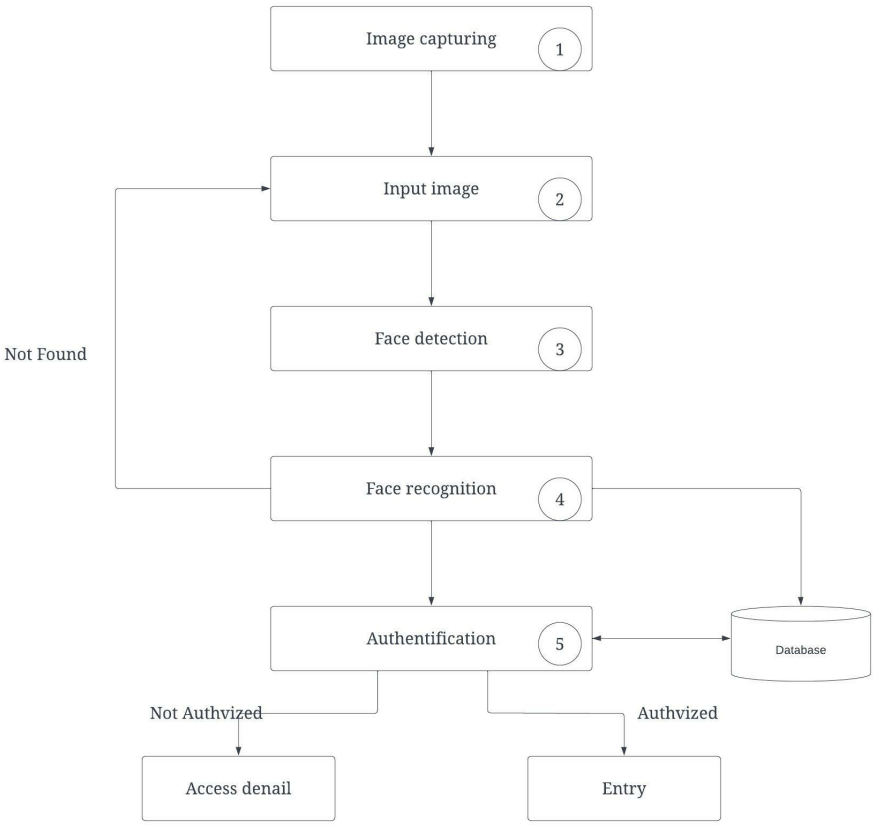

Figure 3.1: Our system overview

3.3 Database design

For the realization of our system we used MySQL Server 2.4.38 and the database named "access_control_system" contains one of the tables "athutication_person", "zone_allowed" and "person_information" which contains the different fields.

For the system to be able to identify a person, it must have saved their coordinates as well as their image, the latter being saved in a file. And the database then contains the identity of the person.

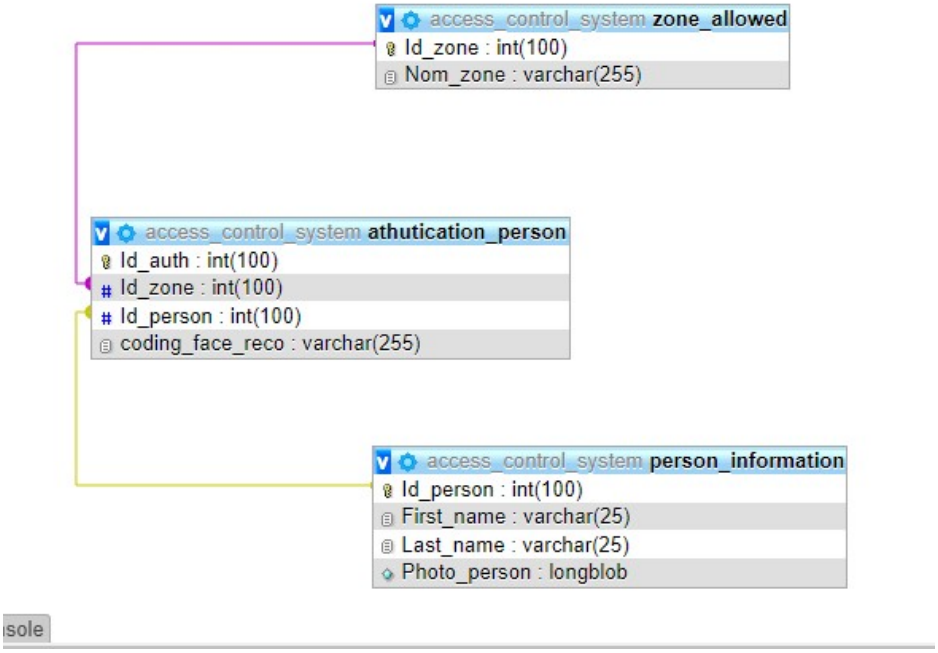

Figure 3.2: Designer Database

3.4 System implementation

Image capturing We used a regular webcam in our work to simulate a surveillance camera.Image is captured in the Following steps:

Step 1: Open and initialize the camera

```
Step 1

#Step 1: Open Webcam
cap=cv2.VideoCapture(0)
```

Figure 3.3: Open and initialize the camera

Step 2: Read an image (one frame) from the camera live video stream

```
Step 3

#Step 3: Read photos from the camera
sucess,img = cap.read()
```

Figure 3.4: Read a frame from the camera live video stream

Step 3: Face detection and recognition expects gray-scale images, so we need to convert the image to gray-scale

```
Step 4

#Step 4: Convert to grey image
gray = cv2.cvtColor(img,cv2.COLOR_BGR2GRAY)
```

Figure 3.5: Convert the captured image to gray-scale

3.4.1 Face detection

To detect face position in the image, we use 'mmod human face detector', a CNN face detector that detects faces in an image and returns the position of each facial in the image using the (left,

top, right, bottom) coordinates of the rectangular bounding box.The coordinates of the detected bounding box of the face are used to crop the facial region.

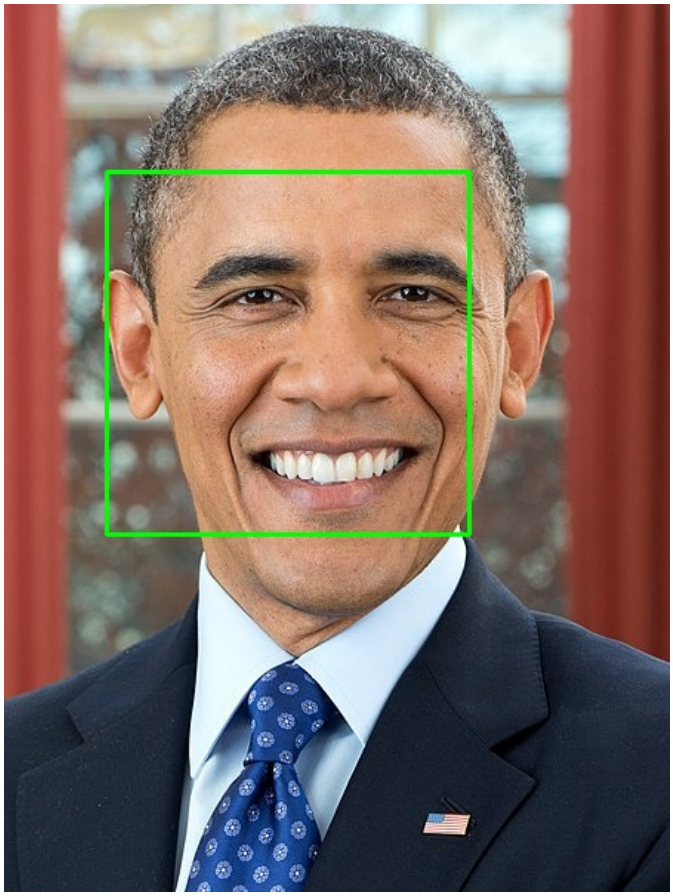

Figure 3.6: Result of face detection [20]

3.4.2 Face recognition

for face recognition steps:

3.4.2.1 Use VGG-face model to create embeddings for faces

For each face/person, we construct embeddings, which define the person in quantitative data. DeepFace, OpenFace, and other pre-trained networks deliver embeddings in less than 5 lines of code. However, we employ VGG Face net to distinguish tagged faces in the wild, which was trained on millions of photos (LFW). The original model uses an image from the WildFace dataset to train VGG face net, which then classifies and recognizes the person in the image.

It generates 2622 embeddings for an image; we use these 2622 embeddings to classify each cropped image later [51].

3.4.2.2 Build Vgg-face architecture and get embeddings for faces

To determine model weights, we must first establish the model architecture. In the output layer, they employed the softmax layer to recognize images in the WildFaces dataset using the VGG Face model in Keras. Only embeddings that are output for the last but one layer are required [51]. The image represents a model VGGFace.

Figure 3.7: Vgg Face model[21]

Next the table indicates the model layering structure

Model: "sequential"		
Layer (type)	Output Shape	Param #
zero_padding2d (ZeroPadding2	(None, 226, 226, 3)	0
conv2d (Conv2D)	(None, 224, 224, 64)	1792
zero_padding2d_1 (ZeroPaddin	(None, 226, 226, 64)	0
conv2d_1 (Conv2D)	(None, 224, 224, 64)	36928
max_pooling2d (MaxPooling2D)	(None, 112, 112, 64)	0
zero_padding2d_2 (ZeroPaddin	(None, 114, 114, 64)	0
conv2d_2 (Conv2D)	(None, 112, 112, 128)	73856
zero_padding2d_3 (ZeroPaddin	(None, 114, 114, 128)	0
conv2d_3 (Conv2D)	(None, 112, 112, 128)	147584
max_pooling2d_1 (MaxPooling2	(None, 56, 56, 128)	0
zero_padding2d_4 (ZeroPaddin	(None, 58, 58, 128)	0
conv2d_4 (Conv2D)	(None, 56, 56, 256)	295168
zero_padding2d_5 (ZeroPaddin	(None, 58, 58, 256)	0
conv2d_5 (Conv2D)	(None, 56, 56, 256)	590080
zero_padding2d_6 (ZeroPaddin	(None, 58, 58, 256)	0
zero_padding2d_6 (ZeroPaddin	(None, 58, 58, 256)	590080
conv2d_6 (Conv2D)	(None, 56, 56, 256)	0
max_pooling2d_2 (MaxPooling2	(None, 28, 28, 256)	0
zero_padding2d_7 (ZeroPaddin	(None, 30, 30, 256)	1180160
conv2d_7 (Conv2D)	(None, 28, 28, 512)	0
zero_padding2d_8 (ZeroPaddin	(None, 30, 30, 512)	2359808
conv2d_8 (Conv2D)	(None, 28, 28, 512)	0
zero_padding2d_9 (ZeroPaddin	(None, 30, 30, 512)	2359808
conv2d_9 (Conv2D)	(None, 28, 28, 512)	0
max_pooling2d_3 (MaxPooling2	(None, 14, 14, 512)	0
zero_padding2d_10 (ZeroPaddi	(None, 16, 16, 512)	2359808
conv2d_10 (Conv2D)	(None, 14, 14, 512)	0
zero_padding2d_11 (ZeroPaddi	(None, 16, 16, 512)	2359808
conv2d_11 (Conv2D)	(None, 14, 14, 512)	0
zero_padding2d_12 (ZeroPaddi	(None, 16, 16, 512)	0
conv2d_12 (Conv2D)	(None, 14, 14, 512)	2359808
max_pooling2d_4 (MaxPooling2	(None, 7, 7, 512)	0
conv2d_13 (Conv2D)	(None, 1, 1, 4096)	102764544
dropout (Dropout)	(None, 1, 1, 4096)	0
conv2d_14 (Conv2D)	(None, 1, 1, 4096)	16781312
dropout_1 (Dropout)	(None, 1, 1, 4096)	0
conv2d_15 (Conv2D)	(None, 1, 1, 2622)	10742334
flatten (Flatten)	(None, 2622)	0
activation (Activation)	(None, 2622)	0
Total params: 145,002,878 Trainable params: 145,002,878 Non-trainable params: 0		

Remove last Softmax layer and get model up to last flatten layer.

we can feed any image to get embeddings which will be used to train our own classi-

last Softmax layer and last flatten layer

```
# Remove last Softmax layer and get model upto last flatten layer #with outputs 2622 units
vgg_face=Model(inputs=model.layers[0].input,outputs=model.layers[-2].output)
```

Figure 3.8: vgg face Model [?]

fier/recognizer.

3.4.2.3 Prepare train data and test data

We prepare train data and test data which contains embeddings as rows for each face and label as person name. Ex: 0: 'nihal', 1: 'aya', ...

Images represent a code for the training of aggregated data

Train Data

```
# Prepare Train Data
x_train=[]
y_train=[]
person_rep=dict()
person_folders=os.listdir(path+'/cropped_face/')
for i,person in enumerate(person_folders):
  person_rep[i]=person
  image_names=os.listdir('cropped_face/'+person+'/')
  for image_name in image_names:
    img=load_img(path+'/cropped_face/'+person+'/'+image_name,target_size=(224,224))
    img=img_to_array(img)
    img=np.expand_dims(img,axis=0)
    img=preprocess_input(img)
    img_encode=vgg_face(img)
    x_train.append(np.squeeze(K.eval(img_encode)).tolist())
    y_train.append(i)
```

Figure 3.9: train data code

Images represent a code for the testing of aggregated data

Test Data

```
# Prepare Test Data
    x_test=[]
    y_test=[]
    person_folders=os.listdir(path+'/images_test_crop/')
    test_image_names=os.listdir('images_test_crop/'+person+'/')
    for image_name in test_image_names:
    img=load_img(path+'/images_test_crop/'+person+'/'+image_name,target_size=(224,224))
        img=img_to_array(img)
        img=np.expand_dims(img,axis=0)
        img=preprocess_input(img)
    img_encode=vgg_face(img)
    x_test.append(np.squeeze(K.eval(img_encode)).tolist())
        y_test.append(i)
```

Figure 3.10: test data code

We previously stored each cropped face image in the corresponding person folder, walked through each folder and in each folder for each image, loaded image from keras in-built function load img(), which is a PIL image with target size=(224,224), because VGG face net expects image shape in (224,224) format, and loaded image from keras in-built function load img(), which is a PIL image with target size=(224 Each loaded image is preprocessed to a scale of [-1,1] and fed into the vgg face() model, which produces a (1,2262) dimensional Tensor, which is then translated to a list and added to the train and test data. In addition, we assign a numerical number to each individual [51].

Convert trained and tested in numpy arrays

```
#Convert trained and tested in numpy arrays
x_train=np.array(x_train)
y_train=np.array(y_train)
x_test=np.array(x_test)
y_test=np.array(y_test)
```

Figure 3.11: train data

And for dataset :Our database contains 100 face images of people, with 2-3 of the same person for some. The images were taken at the same time and with the same lighting condition based on a normal facial expression, but always against a bright background.

Train softmax classifier.

```
#Softmax regressor to classify images based on encoding
classifier_model=Sequential()
#1
classifier_model.add(Dense(units=100,input_dim=x_train.shape[1],kernel_initializer='glorot_uniform'))

classifier_model.add(BatchNormalization())
classifier_model.add(Activation('tanh'))
classifier_model.add(Dropout(0.3))
#2
classifier_model.add(Dense(units=10,kernel_initializer='glorot_uniform'))
classifier_model.add(BatchNormalization())
classifier_model.add(Activation('tanh'))
classifier_model.add(Dropout(0.2))
#3
classifier_model.add(Dense(units=6,kernel_initializer='he_uniform'))
classifier_model.add(Activation('softmax'))
#4
classifier_model.compile(loss=tf.keras.losses.SparseCategoricalCrossentropy(),optimizer='nadam',metri
cs=['accuracy'])
```

Figure 3.12: Train Softmax Classifier

3.4.2.4 Train softmax classifier

Softmax classifier was trained to identify images; it takes face embeddings as input and produces a corresponding image number that is encoded for person name.Next code represents how to train in Python

3.4.2.5 Recognize faces

We can now recognize any face in a picture by using the vgg face model to extract face embeddings, which we can then feed into a classifier to get the person's name. Draw a rectangle box around each face in the image with OpenCV and write the person's name in it. Based on facial cues that identify one face from another, the software generates a facial signature our images:

It accepts the image path and outputs recognized faces in the image with a rectangular box around the face and the name of the person [51].

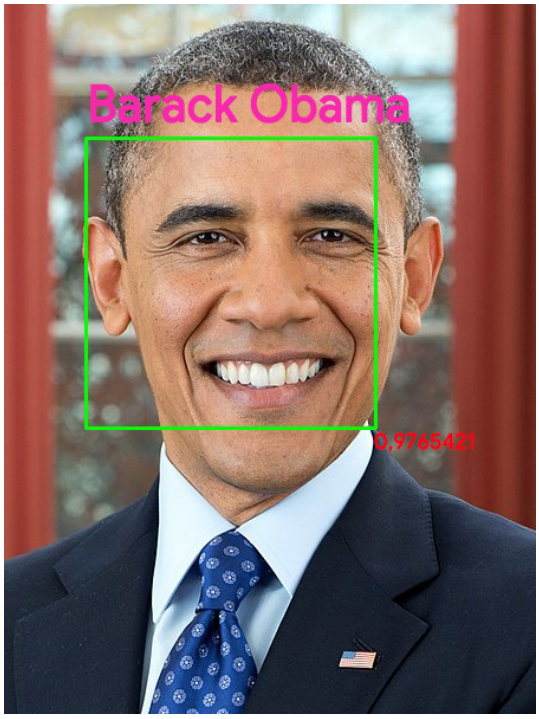

Figure 3.13: Output of face recognition[**?**]

3.4.2.6 Facial signatures compared

A database of known faces is compared to the facial signature (which is essentially simply a mathematical method). This is referred to as 1:n matching (where n equals the number of face signatures in a database).

3.4.2.7 Match or no match decision

If the faceprint acquired matches that of an image in a facial recognition system database, a match/no match judgment is made. Facial recognition software is far from perfect. The accuracy of facial recognition depends on a variety of parameters, including camera quality, light, distance, database size, algorithm, and the subject's ethnicity and gender. False positive error rates (i.e., the system declaring a match erroneously) in advanced systems can be as low as 10% [52].

3.4.3 Authentication

Facial authentication is 1:1, unlike facial recognition, which uses a 1:n match against a database of recognized faces. To secure access to their online account, the user authenticates using their face as a credential. To authenticate, the user just shoots, which is used to build a biometric

template that is compared one-to-one with the stored biometric template. In the background, a proper match based on an accuracy score completes the safe authentication process [52].

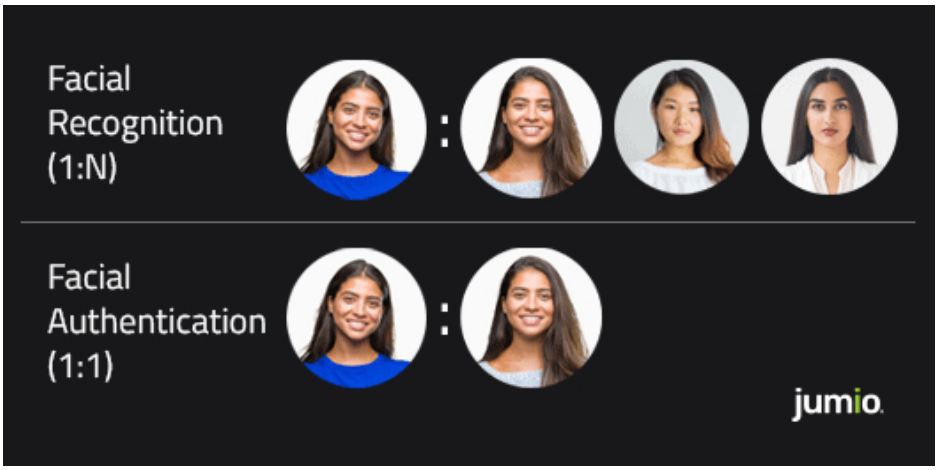

Figure 3.14: face recognition Vs face authentication [22]

After the recognition process,the face verification follows the basic steps:

3.4.3.1 Step01:Create a biometric template

A biometric template is created. Similar to a facial signature, this template is an algorithm that is unique to the user and it's this template that is stored by the business customer for future authentication events.

3.4.3.2 Step02:Issue login credentials (if approved)

The user is vetted by the system and issued login credentials if successfully verified.

3.4.3.3 Step03: Confirm the User's Digital Identity

The user is asked to retake a selfie when they need to enter into their account or complete a high-risk transaction (e.g., a wire transfer or password reset). In seconds, a new biometric template is constructed and compared to the one created during initial enrollment, and a game match determination

3.4.3.4 Step04:Learn from itself

In a process known as adaptive learning, better facial authentication solutions will learn from each authentication occurrence. To improve authentication accuracy and reliability, the new biometric template is compared not only to the initial face map, but also to all future face maps.

3.5 Results

3.5.1 Detection face results

After considering the implementation time in seconds we note that the time gradually decreases after each implementation. We note that the implementation time is great and this will hinder the identification process.
Execution time in seconds 42.83983373641968
Execution time in seconds 33.78818917274475
Execution time in seconds 33.73492383956909
Execution time in seconds 32.461825132369995
Execution time in seconds 30.391246557235718
Execution time in seconds 30.167460203170776
Execution time in seconds 29.19374179840088
Note for accessibility results we did not get because we did not complete this part of the programming. The accuracy of the identification was between 92% and 98%.

3.6 Software environment

3.6.1 Programming language

We chose python as the programming language,it is a high-level and the most commonly used language in data science and deep learning, which is why we chose it with their libraries.

3.6.1.1 Python libraries

NumPy NumPy stands for "Numerical Python" is an open-source package for the Python programming language. It is a library consisting of multidimensional array objects, along with a large collection of high-level mathematical functions to operate on these arrays. In our work, we have installed NumPy 1.22.4 [53].

TensorFlow TensorFlow is an open-source library for fast numerical computing which implements machine learning methods based on deep neural networks (deep learning). At a high level, TensorFlow is a Python library that allows users to express arbitrary computation as a graph of data flows. We have installed TensorFlow 2.9.1 [53].

Keras Keras is a deep learning API written in Python, and its development purpose is to make developing DL models as fast and easy as possible. Keras is used as the back-end of TensorFlow and Theano. In the implementation part of this work, we have used Keras 2.9.0 with the TensorFlow back-end [53].

OpenCV OpenCV (Open Source Computer Vision Library) is an open source computer vision and machine learning software library. OpenCV was built to provide a common infrastructure for computer vision 4.6.0 applications and to accelerate the use of machine perception in the commercial products. Being a BSD-licensed product, OpenCV makes it easy for businesses to utilize and modify the code [54].

3.7 Conclusion

In this chapter, we have described the stages of the design of the recognition system, the hardware and software environment, as well as the details of the realization of our developed system. In view of what has been done in the design and realization, it can be said that:

The system is very interactive, indeed in addition to the recognition with These two methods, it also allows to add new people to the database.
The system performs well due to the good recognition rates.
The system is simple that anyone with little knowledge about biometrics can use it.
The recognition is very fast, since our database is not large.

General Conclusion

In this thesis, we are interested in the problem of access control based on facial recognition.Our work consists in the development of a system intended to recognize an individual by his face using the Convolutional Neural Network method.CNN is one of the most effective methods as a feed-forward network with the power to extract topological properties from the image.

First of all, we made a brief review of the different detection and recognition techniques developed in recent years, and this to highlight facial recognition with its different approaches,then we focus on deep learning used in facial recognition who presents a good performance in classifying known people. Despite all the progress that has been made, problems with pose, lighting, and identification; in outdoor environments; challenges remain that will stimulate the efforts of researchers.

Given the emerging need to use access control applications,face recognition has emerged as an active area of research, spanning disciplines such as image processing,pattern recognition, and computer vision.The existence of other biometric methods does not prevent facial recognition from remaining a powerful and much more widely used tool, because the latter has many more advantages such as ease of use,acceptance by the user and low cost.

The perspectives of this work are many: first, we want to develop a face detection module and just take the square that contains the face into consideration and try from this am deractnier and make it automatic (extraction of the essential points of the eyes, nose, mouth, etc.) Because our system only processes front views; which represent a fixed domain; it would be interesting to define a variable domain covering the variety of lighting conditions, postures and facial expressions.

Bibliography

[1] C. D. Jensen, *Un modèle de contrôle d'accès générique et sa réalisation dans la mémoire virtuelle répartie unique Arias*. PhD thesis, Université Joseph-Fourier-Grenoble I, 1999.

[2] eletelseguranca, "A importância do controle de acesso na gestão do condomínio." https://eletelseguranca.com.br/troubleshoot-electrical-equipment/.

[3] J. Horsey, "Diy real-time raspberry pi face recognition system." https://www.geeky-gadgets.com/raspberry-pi-face-recognition-15-04-2019/.

[4] J. Roldán, "El olimpo en la tierra." https://eldataista.wixsite.com/dataistericos/post/de-seres-humanos-a-dioses.

[5] microcontrollerslab, "Voice recognition system using microcontroller." https://microcontrollerslab.com/voice-recognition-system-using-microcontroller/.

[6] H. Hatem, Z. Beiji, and R. Majeed, "A survey of feature base methods for human face detection," *International Journal of Control and Automation*, vol. 8, pp. 61–78, 2015.

[7] M. Wang and W. Deng, "Deep face recognition: A survey," *Neurocomputing*, vol. 429, pp. 215–244, 2021.

[8] lebanonfiles. https://www.lebanonfiles.com/articles/%D9%85%D8%AA%D9%81%D8%B1%D9%82%D8%A7%D8%AA/%D8%A7%D9%84%D8%A3%D8%B3%D8%A6%D9%84%D8%A9-%D8%A7%D9%84%D8%A3%D9%83%D8%AB%D8%B1-%D8%AA%D8%AF%D8%A7%D9%88%D9%84%D8%A7%D9%8B-%D8%AD%D9%88%D9%84-%D8%B4%D9%8A%D8%AE%D9%88%D8%AE%D8%A9-%D8%A7%D9%84%D8%A8/.

[9] I. Wexler's World, "Age progression." https://www.flickr.com/photos/wexlersworld/3759351256/. July 26, 2009.

[10] sozoclinic, "Signs of aging and how to reverse it." https://sozoclinic.sg/signs-of-aging-the-most-obvious-signs-and-how-to-reverse-it/.

[11] artstation, "1800+ expressions reference pack for artists." https://www.artstation.com/marketplace/p/mel0/1800-expressions-reference-pack-for-artists.

[12] S. Anwarul and S. Dahiya, *A Comprehensive Review on Face Recognition Methods and Factors Affecting Facial Recognition Accuracy*, pp. 495–514. 01 2020.

[13] D. Little, S. Krishna, J. Black, and S. Panchanathan, "A methodology for evaluating robustness of face recognition algorithms with respect to variations in pose angle and illumination angle," *Proceedings. (ICASSP '05). IEEE International Conference on Acoustics, Speech, and Signal Processing, 2005.*, vol. 2, pp. ii/89–ii/92 Vol. 2, 2005.

[14] S. Management. https://www.najmk.com/21370, 07 2018.

[15] A. Magdy. https://www.filfan.com/news/60901, 12 2016.

[16] S. Bharadwaj, H. Bhatt, M. Vatsa, R. Singh, and A. Noore, "Quality assessment based denoising to improve face recognition performance," pp. 140–145, 06 2011.

[17] A. Adel. https://alwafd.news/%D9%85%D9%86%D9%88%D8%B9%D8%A7%D8%AA/3316981-%D8%B5%D9%88%D8%B1-%D8%A8%D8%B3%D9%85%D8%A9-%D8%A8%D9%88%D8%B3%D9%8A%D9%84-%D9%82%D8%A8%D9%84-%D9%88%D8%A8%D8%B9%D8%AF-%D8%B9%D9%85%D9%84%D9%8A%D8%A7%D8%AA-%D8%A7%D9%84%D8%AA%D8%AC%D9%85%D9%8A%D9%84-%D9%84%D9%86-%D8%AA%D8%B5%D8%AF%D9%82-%D8%B4%D9%83%D9%84%D9%87%D8%A7. 17/11/2020.

[18] I. Butma. https://mawdoo3.com/%D8%A3%D8%B6%D8%B1%D8%A7%D8%B1_%D8%A7%D9%84%D9%83%D9%88%D9%84%D8%A7%D8%AC%D9%8A%D9%86_%D9%84%D9%84%D8%A8%D8%B4%D8%B1%D8%A9. 11/03/2017.

[19] P. Fernández. https://rolloid.net/20-imagenes-del-antes-y-despues-de-personas-

[20] wikipedia. https://fr.wikipedia.org/wiki/Fichier:President_Barack_Obama_%28cropped%29.jpg.

[21] sefiks, "Deep face recognition with keras." https://sefiks.com/2018/08/06/deep-face-recognition-with-keras/. August 6, 2018.

[22] D. Nicolls, "Facial identification explained: Face recognition vs. facial authentication." "https://www.jumio.com/facial-recognition-vs-facial-authentication/". July 09, 2019.

[23] L. Ruiqin, T. Wenan, C. Zhenyu, *et al.*, "Design of face recognition access entrance guard system with mask based on embedded development," in *Journal of Physics: Conference Series*, vol. 1883, p. 012156, IOP Publishing, 2021.

[24] G. Boesch. https://viso.ai/deep-learning/vgg-very-deep-convolutional-networks

[25] C. D. Jensen, *Un modèle de contrôle d'accès générique et sa réalisation dans la mémoire virtuelle répartie unique Arias*. PhD thesis, Université Joseph-Fourier-Grenoble I, 1999.

[26] A. MATALLAH, A. BABAHADJ, M. KADDI, *et al.*, *SYSTÈME DE CONTROLE D'ACCES PHYSIQUE*. PhD thesis, Université Ahmed Draïa-Adrar, 2017.

[27] R. Ausanka-Crues, "Methods for access control: advances and limitations," *Harvey Mudd College*, vol. 301, p. 20, 2001.

[28] M. C. Alexander S. Gillis, Peter Loshin, "biometrics." https://www.techtarget.com/searchsecurity/definition/biometrics. July 2021.

[29] Y. J. V. R. Ylber Januzaja, Artan Lumaa, "Real time access control based on face recognition," June 10-11, 2015.

[30] T. Tran and N. Tkauc, "Face recognition and speech recognition for access control," 2019.

[31] C. Bernstein", "face detection." https://www.techtarget.com/searchenterpriseai/definition/face-detection. February 2020.

[32] D. Dwivedi, "Face detection for beginners." https://towardsdatascience.com/face-detection-for-beginners-e58e8f21aad9. Apr 27, 2018.

[33] B. Khefif, "Mise au point d'une application de reconnaissance faciale," *Université Abou Bakr Belkaid–Tlemcen*, vol. 28, 2013.

[34] R. Ullah, H. Hayat, A. A. Siddiqui, U. A. Siddiqui, J. Khan, F. Ullah, S. Hassan, L. Hasan, W. Albattah, M. Islam, *et al.*, "A real-time framework for human face detection and recognition in cctv images," *Mathematical Problems in Engineering*, vol. 2022, 2022.

[35] T. Schenkel, O. Ringhage, and N. Branding, "A comparative study of facial recognition techniques: With focus on low computational power," 2019.

[36] R. Campillo, "Facial recognition history." `https://www.mobbeel.com/en/blog/facial-recognition-history/`. Nov 23, 2020.

[37] R. Ribeiro, D. Lopes, and A. Neves, "Access control in the wild using face verification," in *Intelligent Video Surveillance*, pp. 1–18, IntechOpen, 2018.

[38] kaspersky, "what is facial recognition." `https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition`.

[39] D. N. Parmar and B. B. Mehta, "Face recognition methods & applications," *arXiv preprint arXiv:1403.0485*, 2014.

[40] S. Karamizadeh, S. M. Abdullah, and M. Zamani, "An overview of holistic face recognition," *IJRCCT*, vol. 2, no. 9, pp. 738–741, 2013.

[41] Y. Li and S. Cha, "Face recognition system," *arXiv preprint arXiv:1901.02452*, 2019.

[42] I. Benamiour, S. E. Biad, *et al.*, *Mise au point d'un système de reconnaissance de visage basée Arduino*. PhD thesis, Université de Jijel, 2019.

[43] H. Khalajzadeh, M. Mansouri, and M. Teshnehlab, "Face recognition using convolutional neural network and simple logistic classifier," in *Soft computing in industrial applications*, pp. 197–207, Springer, 2014.

[44] J. Brownlee, "How deep learning works in face recognition?." `https://www.hitechnectar.com/blogs/deep-learning-face-recognition/`.

[45] K. Taylor, "How to perform face recognition with vggface2 in keras." `https://machinelearningmastery.com/how-to-perform-face-recognition-with-vggface2-convolutional-neural-networ` June 5, 2019.

[46] J. K. MERRIN MARY SOLOMON, MAHENDRA SINGH MEENA, "Challenges in face recognition systems," *ijrar*, vol. 6, no. 2, April 10, 2019.

[47] K. Mishra, "Challenges faced by facial recognition system." https://www.pathpartnertech.com/challenges-faced-by-facial-recognition-system/. August 18, 2020.

[48] R. H. A. A. M. Madan Lal, Kamlesh Kumar, "Study of face recognition techniques: A survey," *IJACSA*, vol. 9, No. 6, 2018.

[49] M. C. Agamez, "Aging effects in automated face recognition." https://docs.lib.purdue.edu/open_access_theses/930/. 8-2016.

[50] C. Rathgeb, A. Dantcheva, and C. Busch, "Impact and detection of facial beautification in face recognition: An overview," *IEEE Access*, vol. 7, pp. 152667–152678, 2019.

[51] L. N. Santha, "Face recognition with vgg-face in keras.." https://medium.com/analytics-vidhya/face-recognition-with-vgg-face-in-keras-96e6bc1951d5. Oct 16, 2019.

[52] D. Nicolls, "Facial identification explained: Face recognition vs. facial authentication." https://www.jumio.com/facial-recognition-vs-facial-authentication/.

[53] A. Rao, "Top 10 python libraries you must know in 2022." https://www.edureka.co/blog/python-libraries/. Apr 09,2022.

[54] OpenCv. https://opencv.org/.