

الجمهورية الجزائرية الديمقراطية الشعبية  
وزارة التعليم العالي والبحث العلمي

UNIVERSITÉ BADJI MOKHTAR - ANNABA  
BADJI MOKHTAR – ANNABA UNIVERSITY



جامعة بادجي مختار – عنابة

Faculté : de TECHNOLOGIE

Département : Electronique

Domaine : Sciences et Techniques

Filière Electronique

Spécialité : Electronique système embarqué

## Mémoire

Présenté en vue de l'obtention du Diplôme de Master

Thème :

**Security system based on face recognition**

Présenté par : *latreche Mohamed takieddine.*

*Djellaili naoufel*

### Jury de Soutenance :

BOUTERAA NADIA	MCA	Université UBMA	Président
ZERMI NARIMA	MCA	Université UBMA	Encadrant
HAFS TOUFIK	MCA	Université UBMA	Examineur

Année Universitaire : 2021/2022

# *acknowledgement*

I would like to thank the following people, without whom I would not have been able to complete this research, and without whom I would not have made it through my master degree!

The professors at badji mokhtar University and the electronic department, especially to my supervisor Dr ZERMI NARIMA., whose insight and knowledge into the subject matter steered me through this research.



## ABSTRACT

This whole Project is based on a specific idea that manifest itself in security which it uses the face recognition attribut in making it more efficient and for doing so we will use a particular software appeare in opencv and phyton along a hardware that show up in raspberry pi Just to make the system Works.

## Résumé

L'objectif de projet est basé sur une idée spécifique qui se manifeste dans la sécurité et qui utilise l'attribut de reconnaissance du visage pour le rendre plus efficace. Pour ce faire, nous utiliserons un logiciel particulier appelé opencv et phyton ainsi qu'un matériel appelé raspberry pi pour faire fonctionner le système.

## ملخص

يعتمد هدف المشروع على فكرة محددة تتجلى في الأمان وتستخدم خاصية التعرف على الوجوه لجعلها أكثر فعالية. للقيام بذلك، سنستخدم برنامجًا معينًا يسمى opencv و Phyton بالإضافة إلى أجهزة تسمى raspberry pi لتشغيل النظام.



## figures Table:

1- General Systems Theory schema " <b>analysis-design-develop- implement</b> " .....	3
2- <i>example of physical security systems on the streets</i> .....	7
3- <i>example of physical security system at home</i> .....	8
4- <i>physical security system at buildings</i> .....	10
5- The general scheme of information security threats Classification.....	12
6 - architecture of ANN.....	23
7- Decision Tree schema.....	25
8- EIGENFACES architecture .....	26
9- The ANFIS general Architecture.....	28
10- image illustrates the above extraction.....	34
11- cameras.....	37
12 - circuit diagram.....	40
13 - Raspberry Pi configuration.....	41
14 - Raspberry Pi configuration tool.....	42



## Table des matières

### Chapitre I: security system

<b>I.1</b> security system's Introduction .....	1
<b>I.2</b> security system's history .....	2:3:4
<b>I.3</b> significance of security system :.....	5
1- Assets Protection .....	5
2 -Instant security updates .....	5
3 -Protection when premises or home and your personal data are Unattended .....	5
4 -Conflict resolution .....	5
5 -Value for money .....	6
6 -Monitoring high-risk areas .....	6
7 -Automation and analytics .....	6
<b>I.4</b> types of security systems .....	
<b>I.4.1</b> physical security systems:	
<b>I.4.1.1</b> physical security definition : .....	6
<b>I.4.1.2</b> physical security systems applications .....	7
<b>I.4.1.3</b> At home .....	8
<b>I.4.1.4</b> physical security system existence in buildings.....	8
<b>I.4.2</b> cyber security system .....	9 :10 :11

### Chapitre II : face recognition system

<b>II.1</b> Introduction .....	15
<b>II.2</b> History and elevation of face recognition system.....	17:19
<b>II.3</b> General understanding of facial recognition software	



Works.....	20
------------	----

#### **II.4 Types of face recognition system algorithms :**

1- Deep Learning.....	21:22
2- Decision Tree.....	24
3- Decision Tree Terminologies.....	24
4 -CONVOLUTIONAL NEURAL NETWORK (CNN).....	25
5- EIGENFACES .....	26
6- FISHERFACES.....	26:27
7 -ANFIS.....	28
8- OpenCV.....	29:31
9 -LBPH algorithm (Local Binary Pattern Histogram).....	32

#### **II.5 ADVANTAGES AND DISADVANTAGES OF FACE recognition**

System :

II.5 .1 ADVANTAGES OF FACE RECOGNITION SYSTEM:.....	35
II.5 .2 DISADVANTAGES OF FACE RECOGNITION SYSTEM.....	35

#### **II.6 Cameras**

II.6.1 General definition of camera.....	35
II.6.2 Types of cameras .....	36
1- 2D Camera .....	36
2- 3D camera.....	36



## Chapitre III : application and results

<i>III.introduction.....</i>	<i>39</i>
<i>III.2 Components Required .....</i>	<i>39</i>
<i>III.3 Circuit Diagram.....</i>	<i>40</i>
<i>III.4 Installing OpenCV in Raspberry Pi 3.....</i>	<i>41:44</i>
<i>III.5 coding for Face Recognition Door Lock .....</i>	<i>45:50</i>
<i>III.6 Testing the Raspberry Pi Face Recognition Door Lock.....</i>	<i>51</i>
<i>III.7 The complete code .....</i>	<i>52 :55</i>
<i>III.8 Conclusion.....</i>	<i>55</i>
<b>general Conclusion.....</b>	<b>57</b>
<b>Bibliographie.....</b>	<b>58</b>



## Introduction Générale

Since day one the desire for personal safety and security has been with us and for millennia people would rig branches and rocks and other natural features and fire and night watches to protect themselves from enemies and wild animals to alert them when someone unexpected was coming. And when it comes to the modern Security as a whole is the protection of people, hardware, software, network information and data from physical actions and cyberthreats, intrusions and other events that could damage an organization and its assets. And the most basic definition of any security system is found in its name, it is literally a means or method by which something is secured through a system of interworking components and devices. Which is based on a hardware system that prevents unauthorized intrusion into a premises, and reports such attempts beside a similar software system that prevents unauthorized access.

security camera that has facial recognition in nowadays has improved drastically in the past decade and now it is primarily used for surveillance and security purpose and got spread widely therefor, it has a big potential in an enormous range of fields like: in airports, in crowd management also in grocery stores, and so on. Facial recognition has applications just about everywhere including your home security system. And for my project I would put it on practice in home security system field and specifically "Face Recognition Door Lock System" which is advanced option that lets you make a database of people who visit your house regularly. Then, when the camera sees a face, it determines whether or not it belongs to someone in your list of known faces. If the recognition system does not know who is at the door, it won't open for my project i have settled a specific structure that i will work upon which contain three chapters the first one under the name " security system " and the second chapter is called " face recognition" then the third one which is named " application and results" and after that i go from the chapters off to the general conclusion



## Chapitre I : security system

### Chapitre I: security system

#### I.1 security system's Introduction

#### I.2 security system's history

#### I.3significance of security system :

- 1- Assets Protection
- 2 -Instant security updates
- 3 -Protection when premises or home and your personal data are unattended
- 4 -Conflict resolution
- 5 -Value for money
- 6 -Monitoring high-risk areas
- 7 -Automation and analytics

#### I.4 types of security systems

##### I.4.1 physical security systems:

- 1- *physical security definition :*
- 2 - *physical security systems applications*
- 3 - *At home*
- 4 -*physical security system existence in buildings:*

##### I.4.2cyber security system

### I .1 security system's Introduction:

**Security** refers to all the measures that are taken to protect a place or a thing or a person and something being secured it means that there is a feeling of being safe and free from and also the freedom from risk or danger. The definition is extended by defining risk as the potential loss resulting from the balance of threats, vulnerabilities, countermeasures, and value.

human in order to bring ease to his life he tried hardly to create **systems** that helps in doing so, which are a set of related parts for which there is sufficient coherence between the parts to make viewing them as a whole useful. If we consider more complex situations in which the parts of a system can also be viewed as systems, we can identify useful common systems concepts to aid our understanding. This allows the creation of systems theories, models and approaches useful to anyone trying to understand, create or use collections of related things, independent of what the system is made of or the application domain considering it.....[1]

Specially embedded systems which is a microprocessor- or microcontroller-based system of hardware and software designed to perform dedicated functions within a larger mechanical or electrical system at the core is an integrated circuit designed to carry out computation for real-time operations.

by combining **security and systems** that leads us toward *security system as a whole* that we can say it is a collaboration between a set of related parts such hardware system” like sensors” and similar software system “the code lines that written in a specific programming language” which means it is a network of integrated devices and components that work together to monitor suspicious activity and do a counter against the activity. The devices are connected to a control panel which is basically the hub of the system where the main functions are located. And any of various means or devices designed to guard persons and property in order to protect it from a broad range of hazards, including crime, fire, accidents, espionage, sabotage, subversion, and attack Security systems are found in a wide variety of organizations, ranging from government agencies and industrial plants to apartment buildings and schools. Sufficiently large organizations may have their own proprietary security systems or may purchase security services by contract from specialized security organizations.

### I .2 security system's history

As soon as humans first began having things of value, they wanted to guard it. Our early ancestors who spent a lot of time in caves did set up an early primitive **security**, which they would be well and truly involved in. They used rocks, branches and whatever they could wield to defend their areas and property. Later when wolves were domesticated around 30,000 years ago in some parts of the world, they came to guard the home. In latter times came the guard dog which is still a form of security both for the home and business

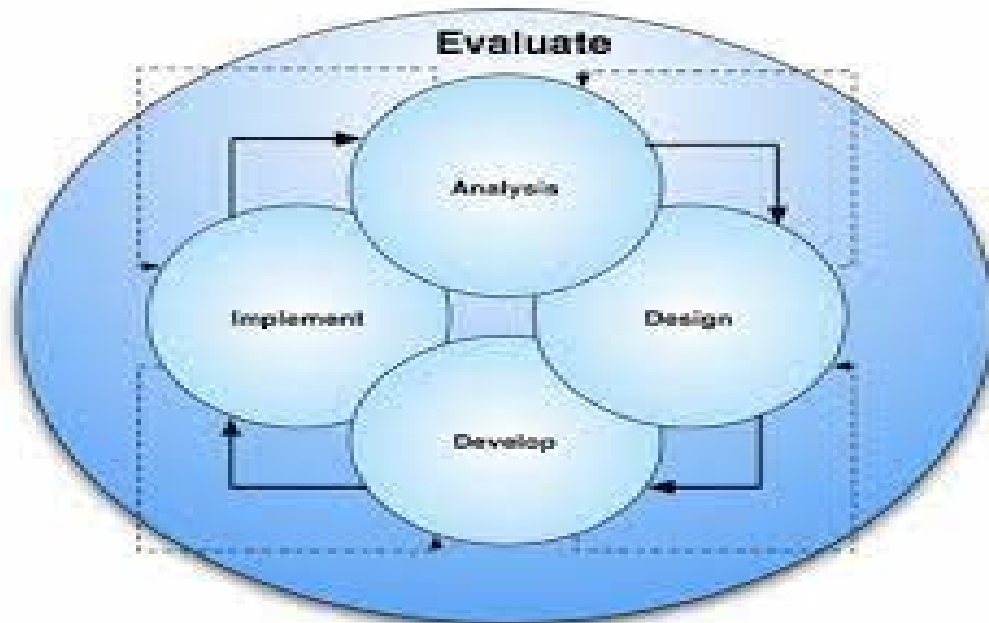
Security by its own definition is the state of being free from danger or threat. A concept that is I feel sometimes forgotten in the hustle and bustle of daily life in this modern world. we can go back in time to see early examples in the Ancient Egyptian Pharaohs who hired private security guards for personal protection. Or to Ancient Rome where emperors had security guards for personal, family and property security. ....[2]

When the Romans came around, they replaced wooden locks with metal and Designed as a burglar deterrent, it ensured that whatever was secured could only be opened with the correct key. This padlock was made of bronze, had patterns on it and was usually shaped into the face of a god. Many Romans, especially rich ones, kept guard dogs to guard their villas and shops. Going up to the Middle Ages when a number of security measures like the crossbow, arrow, moat and bridge to stop intruders getting across, along with high walls to make it hard for intruders to get in. all along with advancements in science and electricity in the 1800s, early alarm systems were invented here in the 21's thanks to advancements in science and technology, security has come a long way. We now live with many different forms of digital security that help keep us and our property safe .....[3]

And in order to make life suitable human tried hard to figure and put a **system** out to put that on display so Since the beginning in the 1950s, when people like Ludwig von Bertalanffy and Kenneth Boulding developed the field of 'General Systems Theory' This theory contributed to the emergence of a new scientific paradigm based on the interrelationship between the constituent elements of systems. Previously it was held that systems as a whole were equal to the sum of their parts, and that they could be studied from the individual analysis of their components. Since its inception, general systems theory has been applied to biology, to psychology, mathematics, computational sciences, economics, sociology, politics

## Chapitre 1: security system

and other exact and social sciences, especially in the context of the analysis of interactions. and that leads us to the base of *the modern system which its backbone is this theory*. Which mean that it is a set of related parts for which there is sufficient coherence between the parts to make viewing them as a whole useful for us.



**Figure (1):** General Systems Theory schema "**analysis-design-develop-implement**"

*Featuring the two concepts of **security and system*** that put us in the right way to put the light on the history of *security system* as a whole that its most basic level, personal security can be argued as beginning in the stone age, which began some 2.5 million years ago in Africa when our distant relatives began creating tools and weapons out of stone and organic material including wood, leather, and bone. The stone age is a time when small tribes of people and whatever weapons they had at their disposal were the only sources of security when the unexpected might happen. Arrows, spearheads, and knives were some of the most common tools created during the stone age.

The stone age lasted more than 90% of human existence and ended around 3,000 BC when the Bronze Age started. This period lasted from 3,000-1,000 BC and replaced the stone age when bronze (a mixture of copper and tin) was used in place of stone, wood, leather etc. to make tools and weapons. Bronze swords, daggers, and axes replaced stone weapons and brought about a significant cultural shift.

## Chapitre 1: security system

The bronze age ended around 1,000 BC when the Iron Age began, which brought more significant cultural changes as well, the most significant change being weaponry. Two-horse iron chariots changed the game in battles when heavily armored soldiers needed to get in and out of the battlefield quickly. Javelins, spears, small swords and daggers were the weapons of choice in the early Iron Age. After the Iron Age, many periods follow including the Roman era, medieval era, and more which all lead up to present day, 21st century. All of these different eras had one thing in common though: they each presented new technologies that brought about a cultural shift. We are currently in the midst of such a shift as we see Artificial Intelligence (AI) disrupting every industry, including security.

We're optimistic about the future of business security, but we've said it before and we'll say it again – there will always be a need to protect your people and your property. We look forward to seeing the effects of AI applications in the security industry in the coming years...[4]

### I .3 significance of security system

Professional Electronic Security Systems have saved billions of dollars and lives since their invention and implementation in residential and business environments. Here are the most important reasons why you must install electronic security on your premises:

**1.Assets Protection:** Electronic security is one of the cheapest prevention measures to protect your business and personal assets such as money, furniture and even intellectual property being under strict non-disclosure conditions. In simple wordstheft.

**2.Instant security updates:** Modern electronic security systems can be accessed through different electronic devices such as computers, tablets or mobile phones. With novel technology and cloud systems, you can be aware of the situation wherever you are: at home, on vacation, or commuting. With instant security alerts on your phone, you can find out about a security breach within seconds.

**3.Protection when premises or home and your personal data are unattended:**

Modern technology implemented in electronic security systems allow you to travel for longer periods of time. Complex security codes and accessibility anywhere in the world can

## Chapitre 1: security system

help protect your business information and assets while you're travelling, electronic security will protect you from both external and internal

**4.Conflict resolution:** Integrated security systems including CCTV security cameras, access control systems, security alarms and security officers can provide important evidence whether a problem arises in the workplace, regardless if it is an internal or external robbery/break-ins or cyber-attack.

**5.Value for money:** Better safe than sorry. Better spend a few hundred dollars than lose thousands. Electronic Security Systems provide value for money and peace of mind.

**6.Monitoring high-risk areas:** it may be placed in areas where risk is high. You can install security systems in places that are vulnerable to vandalism, theft or break ins. People with bad intentions like to target vulnerable areas of your premises, such as those that are poorly lit and look like they have not been well maintained. It gives the perception that those areas are not viewed or seldom attended. These are the ideal hiding spots or viewing spots for them to monitor your business or personal safety

**7.Automation and analytics:** New CCTV technology performs advanced threat detection through facial recognition and spotting potential criminals. Analytical reports and automated systems represent a refined use of resources, making it easier for humans to control any emergency situations.....[5]

### I .4 types of security systems:

when it comes to the types of security systems, we as human have been working on multiple ranks and levels to improve our daily life so that lead us to two basics types which are: physical security - cyber security.

#### I .4.1physical security systems:

##### 1-physical security definition:

Physical security measures are designed to protect buildings, and safeguard the equipment inside and human body. In short, they keep unwanted people out, and give access to authorized individuals. Without physical security plans in place, your office or

## Chapitre 1: security system

building and your personal safety is left open to criminal activity, and liable for types of physical security threats including theft, vandalism, fraud, and even accidents.

In the built environment, we often think of physical security control examples like locks, gates, and guards. While these are effective, there are many additional and often forgotten layers to physical security for offices that can help keep all your assets protected. A comprehensive physical security plan combines both technology and specialized hardware, and should include countermeasures against intrusion.....[6]

### 2-physical security systems applications:

#### *on the streets:*

Physical security involves the use of many layers of interdependent systems that can contain: protective barriers, security guards, locks, access control, CCTV surveillance, perimeter intrusion detection, deterrent systems, protection from fire, Road Blocker and so on.



Figure 2: *example of physical security systems on the streets*

#### **3-At home:**

*There is a significance role for physical security system existence at Home includes both the security hardware placed on a property and individuals' personal security practices. Security hardware includes windows and doors, alarm systems, lighting, locks, motion detectors, and security camera systems*



Figure 3 : *example of physical security system at home*

### **4-physical security system existence in buildings:**

There is a major role for physical security system existence in buildings whether it is company or school, university and so on. Building security and control system have become necessary with increasing size and complexity of buildings. The building security and control system is designed to monitor and control mechanical and electrical installations, fire protection and escape, burglary, assault and emergency communication. In tall buildings and major complexes, the most important security requirement is fire-safety system. In addition to the structural precautions for fire protection, special system is required to monitor and control are:

Fire detection and suppression,

Movement and protection of people

Smoke control including pressurization and barriers

Safe places of refuge and

Emergency arrangements and communication.



## Chapitre 1: security system

In major buildings, these arrangements are integrated with those required to monitor and control the heating, ventilation and air-conditioning systems and other aspects of security within a single electronic system. The computer monitors all significant local conditions and appropriate action is taken.....[7]



**Figure (4):** *physical security system at buildings*

### 1.4.2cyber security system:

**a- Cyber security definition:** Cyber security system is the manifestation of technologies, processes and controls to protect networks, programs, devices and data from cyber-attacks.

## Chapitre 1: security system

It aims to reduce the risk of cyber-attacks and protect against the unauthorized exploitation of systems, networks and technologies. It's also known as information technology security or electronic information security. The term applies in a variety of contexts, from business to mobile computing, and can be divided into a few common categories.....[8]

### **b-Cyber security system applications:**

**Network security:** is the practice of securing a computer network from intruders, whether targeted attackers or opportunistic malware.

**Application security:** focuses on keeping software and devices free of threats. A compromised application could provide access to the data its designed to protect. Successful security begins in the design stage, well before a program or device is deployed.

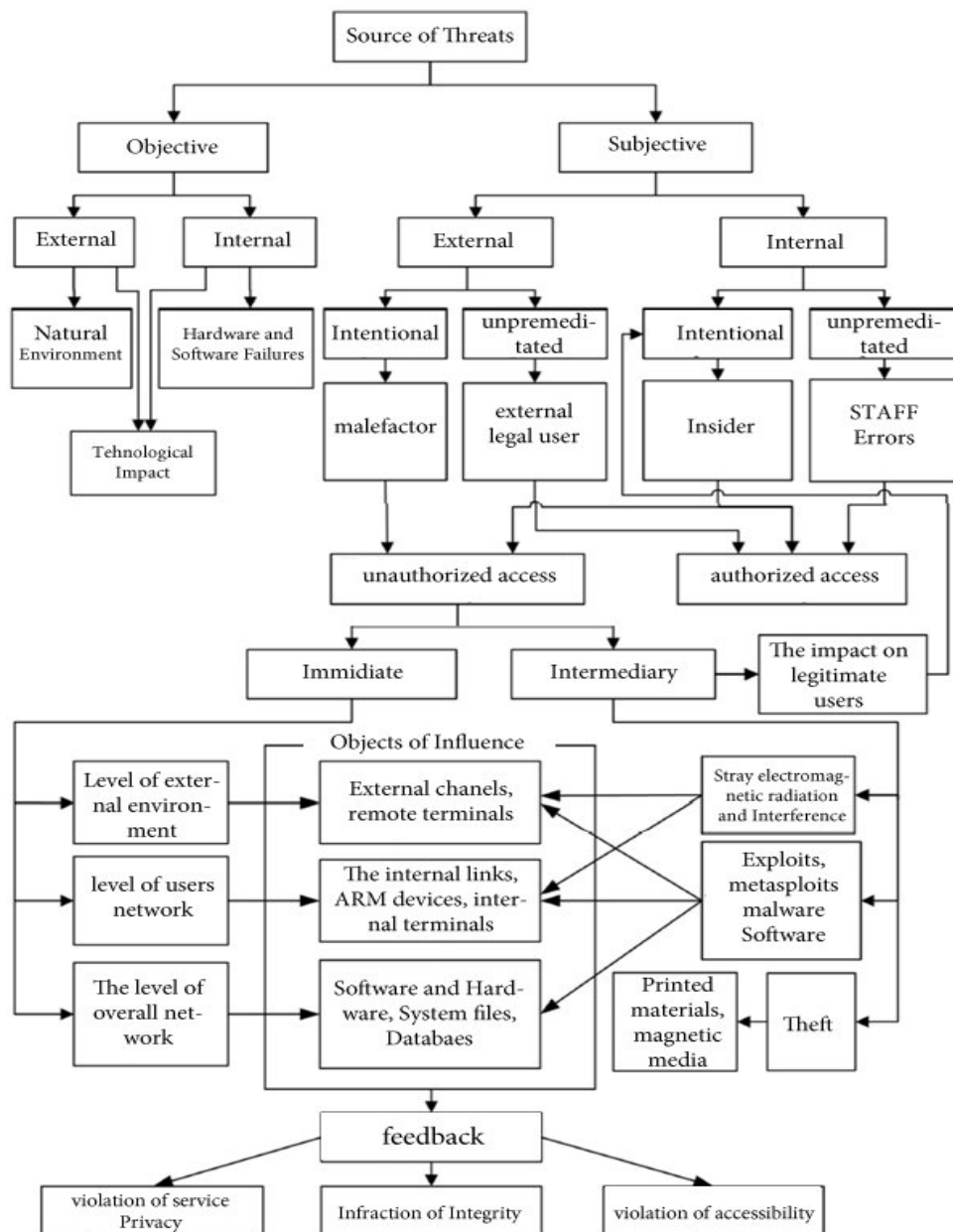
**Information security:** protects the integrity and privacy of data, both in storage and in transit.

**Operational security:** includes the processes and decisions for handling and protecting data assets. The permissions users have when accessing a network and the procedures that determine how and where data may be stored or shared all fall under this umbrella.

**Disaster recovery and business continuity:** define how an organization responds to a cyber-security incident or any other event that causes the loss of operations or data. Disaster recovery policies dictate how the organization restores its operations and information to return to the same operating capacity as before the event. Business continuity is the plan the organization falls back on while trying to operate without certain resources.

**End-user education:** addresses the most unpredictable cyber-security factor: people. Anyone can accidentally introduce a virus to an otherwise secure system by failing to follow good security practices. Teaching users to delete suspicious email attachments, not plug in unidentified USB drives, and various other important lessons is vital for the security of any organization.....[9]

## Chapitre 1: security system



**Figure(5):** The general scheme of information security threats classification

## Chapitre II : face recognition system

Table des matières :

**II.1** *Introduction*

**II.2** *History and elevation of face recognition syst*

**II.3** *General understanding of facial recognition software Works*

**II.4** *Types of face recognition system algorithms*

**II.5** ADVANTAGES AND DISADVANTAGES OF FACE recognition

System :

**II.5 .1** ADVANTAGES OF FACE RECOGNITION SYSTEM:

**II.5 .2** DISADVANTAGES OF FACE RECOGNITION SYSTEM

**II.6** *Cameras*

**II.6.1** General definition of camera

**II.6.2** Types of cameras

### II.1 Introduction :

In recent years, with the demand for better security, computers have played a large role. Due to their precision, large memory banks and high computing power, considerable development has been made in the area of face recognition. Computers now surpass humans in many faces' recognition tasks. A human being can remember limited number of faces. But a computer doesn't have any limits, and can hence be used where large databases of facial records are needed. Such a facial recognition system has many potential applications including crowd and airport surveillance, private security and improved human-computer interaction. Such a system is perfectly suited to fix security issues and offer flexibility to smart house control. This project is aimed to be a complete system for face recognition : easy to build, cheap cost and effective. Main purpose is to be set as an alert for home visitors and provide information about the visitors in a dynamic website and phone application. It can also be used in other fields like industries, offices and even air-ports for identifying wanted people. Among the other bio-metric techniques, face recognition method offers one great advantage which is user friendliness.

A facial recognition system is a technology capable of matching a human face from a digital image or a video frame against a database of faces, typically employed to authenticate users through ID verification services, works by pinpointing and measuring facial features from a given image.

Face recognition play a vital role in variety of applications from biometrics, surveillance, security, identification to the authentication. In this paper we design and implement a smart security system for restricted area where access is limited to people whose faces are available in the training database. First, we are going to detect the face by detecting the human motion. Then face recognition is performed to determine the authority of the person to enter the sensitive area. At the same time, we track the coordinate of detected motion. Failing to recognize the face finally passes the estimated coordinate to anesthetic gun for targeting the intruder automatically. Experimental results demonstrate the effectiveness of proposed security system in order to restrict the unauthorized access and enhanced reliability by use of face recognition.[10]

## Chapitre2: face recognition system

facial recognition systems have seen wider uses in recent times on smartphones and in other forms of technology, such as robotics. Because computerized facial recognition involves the measurement of a human's physiological characteristics, facial recognition systems are categorized as biometrics. Although the accuracy of facial recognition systems as a biometric technology is lower than iris recognition and fingerprint recognition, it is widely adopted due to its contactless process. Facial recognition systems have been deployed in advanced human-computer interaction, video surveillance and automatic indexing of images.....[11]

Face recognition is generally divided into two sub-categories. On the one side, face verification consists in checking if a face corresponds to a given identity. On the other side, face identification consists in finding the identity corresponding to a given face. Face recognition can also be divided in terms of evaluation protocol. Either algorithms are tested under the closed-set protocol or under the open-set protocol. In the former, the testing identities are the same as the training ones and face recognition can then be assimilated to a classification problem. In the latter case, the testing identities are usually disjoint from the training ones. The problem becomes more one of encoding faces into a discriminative feature space .....[12]

### **II.2 History and elevation of face recognition system:**

History and elevation of face recognition system has a deep root back throughout history since the modern technology saw its first day light and from that point along scientists start work on make it more efficient and widely used in our life thus the development took a place at many levels and ranks.

facial recognition was pioneered in the 1960s. Woody Bledsoe, Helen Chan Wolf, and Charles Bisson worked on using the computer to recognize human faces. Their early facial recognition project was dubbed "man-machine" because the coordinates of the facial features in a photograph had to be established by a human before they could be used by the computer for recognition. On a graphics tablet a human had to pinpoint the coordinates of facial features such as the pupil centers, the inside and outside corner of eyes, and the widows peak in the hairline. The coordinates were used to calculate 20 distances, including the width of the mouth and of the eyes. A human could process about 40 pictures an hour in this manner and so build a database of the computed distances. A computer would then

## Chapitre2: face recognition system

automatically compare the distances for each photograph, calculate the difference between the distances and return the closed records as a possible match

In 1970, Takeo Kanade publicly demonstrated a face-matching system that located anatomical features such as the chin and calculated the distance ratio between facial features without human intervention. Later tests revealed that the system could not always reliably identify facial features. Nonetheless, interest in the subject grew and in 1977 Kanade published the first detailed book on facial recognition technology

In 1993, the Defense Advanced Research Project Agency (DARPA) and the Army Research Laboratory (ARL) established the face recognition technology program FERET to develop "automatic face recognition capabilities" that could be employed in a productive real-life environment "to assist security, intelligence, and law enforcement personnel in the performance of their duties." Face recognition systems that had been trialed in research labs were evaluated and the FERET tests found that while the performance of existing automated facial recognition systems varied, a handful of existing methods could viably be used to recognize faces in still images taken in a controlled environment The FERET tests spawned three US companies that sold automated facial recognition systems. Vision Corporation and Miro's Inc were both founded in 1994, by researchers who used the results of the FERET tests as a selling point. Visage Technology was established by an identification card defense contractor in 1996 to commercially exploit the rights to the facial recognition algorithm developed by Alex Pentland at MIT.

Following the 1993 FERET face-recognition vendor test the Department of Motor Vehicles (DMV) offices in West Virginia and New Mexico were the first DMV offices to use automated facial recognition systems as a way to prevent and detect people obtaining multiple driving licenses under different names. Driver's licenses in the United States were at that point a commonly accepted form of photo identification. DMV offices across the United States were undergoing a technological upgrade and were in the process of establishing databases of digital ID photographs. This enabled DMV offices to deploy the facial recognition systems on the market to search photographs for new driving licenses against the existing DMV database DMV offices became one of the first major markets for automated facial recognition technology and introduced US citizens to facial recognition as a standard method of identification. The increase of the US prison population in the 1990s prompted U.S. states to

## Chapitre2: face recognition system

established connected and automated identification systems that incorporated digital biometric databases, in some instances this included facial recognition. In 1999, Minnesota incorporated the facial recognition system Face IT by Visionist into a mug shot booking system that allowed police, judges and court officers to track criminals across the state. In this shear mapping the red arrow changes direction, but the blue arrow does not and is used as eigenvector.

The Viola–Jones algorithm for face detection uses Haar-like features to locate faces in an image. Here a Haar feature that looks similar to the bridge of the nose is applied onto the face. Until the 1990s, facial recognition systems were developed primarily by using photographic portraits of human faces. Research on face recognition to reliably locate a face in an image that contains other objects gained traction in the early 1990s with the principal component analysis (PCA). The PCA method of face detection is also known as Eigenface and was developed by Matthew Turk and Alex Pentland. Turk and Pentland combined the conceptual approach of the Karhunen–Loève theorem and factor analysis, to develop a linear model. Eigenfaces are determined based on global and orthogonal features in human faces.

A human face is calculated as a weighted combination of a number of Eigenfaces. Because few Eigenfaces were used to encode human faces of a given population, Turk and Pentland's PCA face detection method greatly reduced the amount of data that had to be processed to detect a face. Pentland in 1994 defined Eigenface features, including eigen eyes, eigen mouths and eigen noses, to advance the use of PCA in facial recognition. In 1997, the PCA Eigenface method of face recognition was improved upon using linear discriminant analysis (LDA) to produce Fisher faces. LDA Fisher faces became dominantly used in PCA feature based face recognition. While Eigenfaces were also used for face reconstruction. In these approaches no global structure of the face is calculated which links the facial features or parts. Purely feature based approaches to facial recognition were overtaken in the late 1990s by the Bochum system, which used Gabor filter to record the face features and computed a grid of the face structure to link the features. Christoph von der Malsburg and his research team at the University of Bochum developed Elastic Bunch Graph Matching in the mid-1990s

to extract a face out of an image using skin segmentation. By 1997, the face detection method developed by Malsburg outperformed most other facial detection systems on the



market. The so-called "Bochum system" of face detection was sold commercially on the market as ZN-Face to operators of airports and other busy locations. The software was "Robust enough to make identifications from less-than-perfect face views. It can also often see through such impediments to identification as mustaches, beards, changed hairstyles and glasses—even sunglasses". Real-time face detection in video footage became possible in 2001 with the Viola–Jones object detection framework for faces. Paul Viola and Michael Jones combined their face detection method with the Haar-like feature approach to object recognition in digital images to launch AdaBoost, the first real-time frontal-view face detector. By 2015, the Viola–Jones algorithm had been implemented using small low power detectors on handheld devices and embedded systems.....[13]

in every day, there is a new development still in this aspect that keeps improving the production out of the face recognition system.

### **II.3 General understanding of facial recognition software works:**

Most people have seen facial recognition used in movies for decades (video), but it's rarely depicted correctly. Every facial recognition system works differently—often built on proprietary algorithms—but you can sort out the process into three basic types of technology:

*Detection* is the process of finding a face in an image. If you've ever used a camera that detects a face and draws a box around it to auto-focus, you've seen this technology in action. On its own, it isn't nefarious—face detection only focuses on finding a face, not the identity behind it.

*Analysis* is the step that maps faces—often by measuring the distance between the eyes, the shape of the chin, the distance between the nose and mouth—and then converts that into a string of numbers or points, often called a "faceprint." Goofy Instagram or Snapchat filters use similar technology (video). Although analysis can suffer from glitches, particularly involving misidentification, that's generally problematic only when the faceprint is added to a recognition database.

*Recognition* is the attempt to confirm the identity of a person in a photo. This process is used for verification, such as in a security feature on a newer smartphone, or for

## Chapitre2: face recognition system

identification, which attempts to answer the question “Who is in this picture?” And this is where the technology steps into the creepier side of things.

The detection phase of facial recognition starts with an algorithm that learns what a face is. Usually the creator of the algorithm does this by “training” it with photos of faces. If you cram in enough pictures to train the algorithm, over time it learns the difference between, say, a wall outlet and a face. Add another algorithm for analysis, and yet another for recognition, and you’ve got a recognition system.

The diversity of photos fed into the system has a profound effect on its accuracy during the analysis and recognition steps. For example, if the sample sets mostly include white men—as was the case in the training of early facial recognition systems—the programs will struggle to accurately identify BIPOC faces and women. The best facial recognition software has started to correct for this in recent years, but white males are still falsely matched less frequently (PDF) than other groups; some software misidentifies some Black and Asian people 100 times more often than white men. Mutale Nkonde, fellow of the Digital Civil Society Lab at Stanford and member of the TikTok Content Advisory Council, notes that even if the systems are operating perfectly, issues with gender identification remain: “Labels are typically binary: male, female. There is no way for that type of system to look at non-binary or even somebody who has transitioned.”

Once a company trains its software to detect and recognize faces, the software can then find and compare them with other faces in a database. This is the identification step, where the software accesses a database of photos and cross-references to attempt to identify a person based on photos from a variety of sources, from mug shots to photos scraped off social networks. It then displays the results, usually ranking them by accuracy. These systems sound complicated, but with some technical skill, you can build a facial recognition system yourself with off-the-shelf software .....[14]

### **II.4 Types of face recognition system algorithms:**

#### **Machine learning:**

Being a subset of Artificial Intelligence, Machine Learning is the technique that trains computers/systems to work independently, without being programmed explicitly. And,

during this process of training and learning, various algorithms come into the picture, that helps such systems in order to train themselves in a superior way with time, are referred as Machine Learning Algorithms.....[15]

Machine learning is a method of data analysis that automates analytical model building. It is a branch of artificial intelligence based on the idea that systems can learn from data, identify patterns and make decisions with minimal human intervention algorithms use statistics to find patterns in huge amounts of data. This data can include words, numbers, images, clicks, and more.

some of the fascinating machine learning algorithms:

### **1- Deep Learning:**

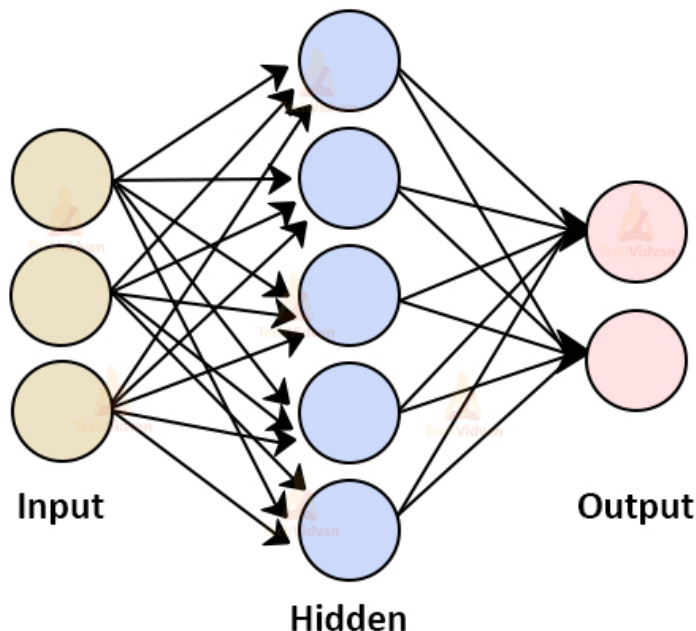
Deep Learning is a subfield of machine learning concerned with algorithms inspired by the structure and function of the brain called artificial neural networks. And subset of a Machine Learning algorithm that uses multiple layers of neural networks to perform in processing data and computations on a large amount of data. Deep learning algorithm works based on the function and working of the human brain.

we can say a type of machine learning based on artificial neural networks in which multiple layers of processing are used to extract progressively higher-level features from data.

The deep learning algorithm is capable to learn without human supervision, can be used for both structured and unstructured types of data. Deep learning can be used in various industries like healthcare, finance, banking, e-commerce and so on Face recognition is the problem of identifying and verifying people in a photograph by their face. It is a task that is trivially performed by humans, even under varying light and when faces are changed by age or obstructed with accessories and facial hair. Nevertheless, it is remained a challenging computer vision problem for decades until recently. Deep learning methods are able to leverage very large datasets of faces and learn rich and compact representations of faces, allowing modern models to first perform as-well and later to outperform the face recognition capabilities of humans. Deep learning methods can achieve superhuman performance....[16]

That use Artificial Neural Networks are a special type of machine learning algorithms that are modeled after the human brain. That is, just like how the neurons in our nervous system are able to learn from the past data, similarly, the ANN is able to learn from the data and provide responses in the form of predictions or classifications. ANNs are nonlinear statistical models which display a complex relationship between the inputs and outputs to discover a new pattern. A variety of tasks such as image recognition, speech recognition, machine translation as well as medical diagnosis makes use of these artificial neural networks. An important advantage of ANN is the fact that it learns from the example data sets. Most commonly usage of ANN is that of a random function approximation. With these types of tools, one can have a cost-effective method of arriving at the solutions that define the distribution. ANN is also capable of taking sample data rather than the entire dataset to provide the output result. With ANNs, one can enhance existing data analysis techniques owing to their advanced predictive capabilities.....[17]

### Architecture of Artificial Neural Network



Figure(6):architecture of ANN

### 2-Decision Tree :

The decision tree is the decision supporting tool that practices a tree-like graph or model of decisions along with their feasible outcomes, like the chance-event outcome, resource costs and implementation. Being a supervised learning algorithm, decision trees are the best choice for classifying both categorical and continuous dependent variables. In this algorithm, the population is split into two or more homogeneous datasets, relying on the most significant characteristics or independent variables.

### 3-Decision Tree Terminologies:

**Root Node:** Root node is from where the decision tree starts. It represents the entire dataset, which further gets divided into two or more homogeneous sets.

**Leaf Node:** Leaf nodes are the final output node, and the tree cannot be segregated further after getting a leaf node.

**Splitting:** Splitting is the process of dividing the decision node/root node into sub-nodes according to the given conditions.

**Branch/Sub Tree:** A tree formed by splitting the tree.

**Pruning:** Pruning is the process of removing the unwanted branches from the tree.

**Parent/Child node:** The root node of the tree is called the parent node, and other nodes are called the child nodes.

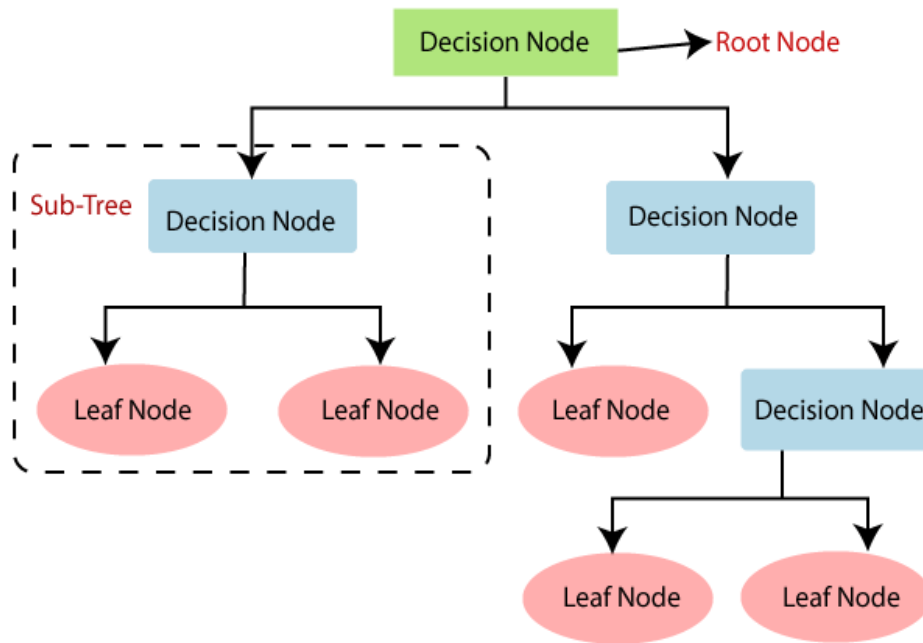


Figure (7): Decision Tree schema

The steps:

Step-1: Begin the tree with the root node, says S, which contains the complete dataset.

Step-2: Find the best attribute in the dataset using Attribute Selection Measure (ASM).

Step-3: Divide the S into subsets that contains possible values for the best attributes.

Step-4: Generate the decision tree node, which contains the best attribute.

Step-5: Recursively make new decision trees using the subsets of the dataset created in step - 3. Continue this process until a stage is reached where you cannot further classify the nodes and called the final node as a leaf node.

### 4-CONVOLUTIONAL NEURAL NETWORK (CNN):

Convolutional neural network (CNN) is one of the breakthroughs of artificial neural networks (ANN) and AI development. It's one of the most popular algorithms in deep learning, a type of machine learning in which a model learns to perform classification tasks directly on an image, video, text, or sound. The model shows impressive results in several fields: computer vision, natural language processing (NLP), and the largest image classification data set (Image Net). CNN is a normal neural network with new layers —

convolutional and pooling. CNN can have dozens and hundreds of these layers, and each of them learns to detect different imaging features.

### 5-EIGENFACES:

Eigenfaces is a face detection and recognition method that determines face variance in image data sets. It uses these variances to encode and decode faces with machine learning. A set of eigenfaces is a collection of “standardized face ingredients” determined by statistical analysis of a large number of face images. Facial features are assigned mathematical values, as this method doesn’t use digital pictures but rather statistical databases. Any human face is a combination of these values with different percentages.....[18]

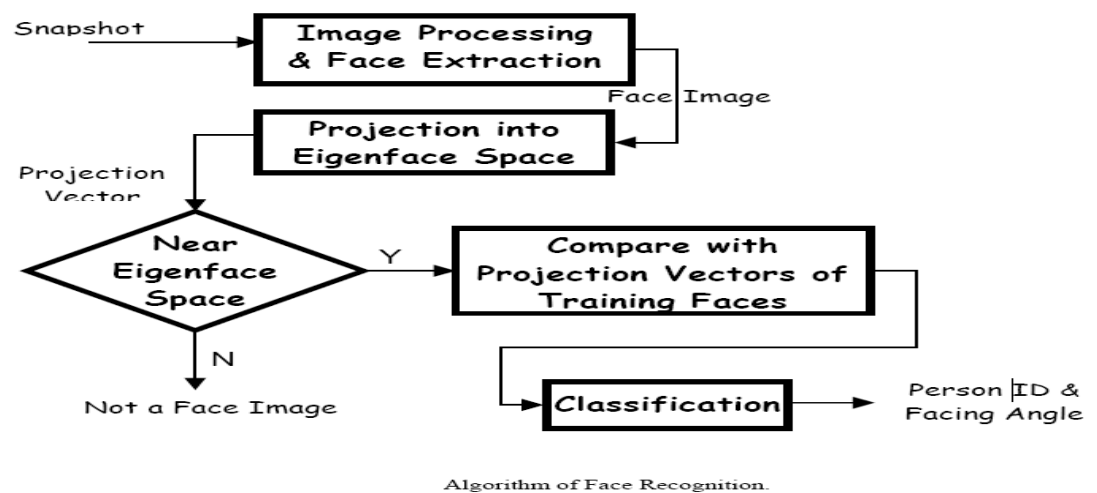


Figure (8): EIGENFACES architecture

### 6-FISHERFACES:

Fisher faces is one of the most popular facial recognition algorithms; it's considered superior to many of its alternatives. As an improvement to the Eigenfaces algorithm, it's often compared to Eigenfaces and considered more successful in class distinction in the training process. The key advantage of this algorithm is its ability to interpolate and extrapolate over lighting and facial expression variation. There are reports of 93% accuracy of the Fisher faces algorithm when combined with the PCA method at the preprocessing stage. Fisher Faces is an improvement over Eigenfaces and uses Principal Component Analysis (PCA) and Linear Discriminant Analysis (LDA).[18]

-Fisher Faces Process:

### Step 1: Retrieve data

Collection of data is done in form of face images. Collection can be done using photographs already saved or from a webcam. Face must be fully visible and must be facing forward.

### Step 2: Image Processing

**a) Preprocessing stage:** Getting images using camera or saved images and conversion from RGB to grayscale. Image data is divided into training and test data.

**b) Processing stage:** Fisher face method will be applied to generate feature vector of facial image data used by system and then to match vector of traits of training image with vector characteristic of test image using Euclidean distance formula

### Step 3: Feature generation

Features of the faces are extracted.

### Recognition process:

After the training is done, the next stage is image recognition process. The goal is to successfully recognize the test image.

If training image is the same as the testing image: In this case system can successfully identify the test image correctly up to 100%.

If training image is not the same as the testing image: The test image and the training image must come from the image of the same person's face. System can now successfully identify the test image correctly up to 90%.....[19]

### 7-ANFIS:

An adaptive neuro-fuzzy interference system (ANFIS) is a type of artificial neural network. This method integrates the principles of neural networks with fuzzy logic principles and combines their advantages in a single structure. ANFIS is used to classify image features extracted from datasets on the preprocessing stage. Data scientists combine this method with a variety of feature extraction algorithms. Thus, some studies reported incredible 97.1%



ANFIS classification accuracy after feature extraction with 2D principal component analysis. The architecture of ANFIS consists of five layers. Each layer contains several nodes described by the node function. Adaptive nodes, denoted by squares, represent the parameter sets that are adjustable in these nodes, whereas fixed nodes, denoted by circles, represent the parameter sets that are fixed in the system. Adaptive Neuro-Fuzzy Inference System (ANFIS) is a neural network functionality equivalent to fuzzy inference system. This architecture has the potentials to capture the benefits of both the neural network and the fuzzy logic in one [18]

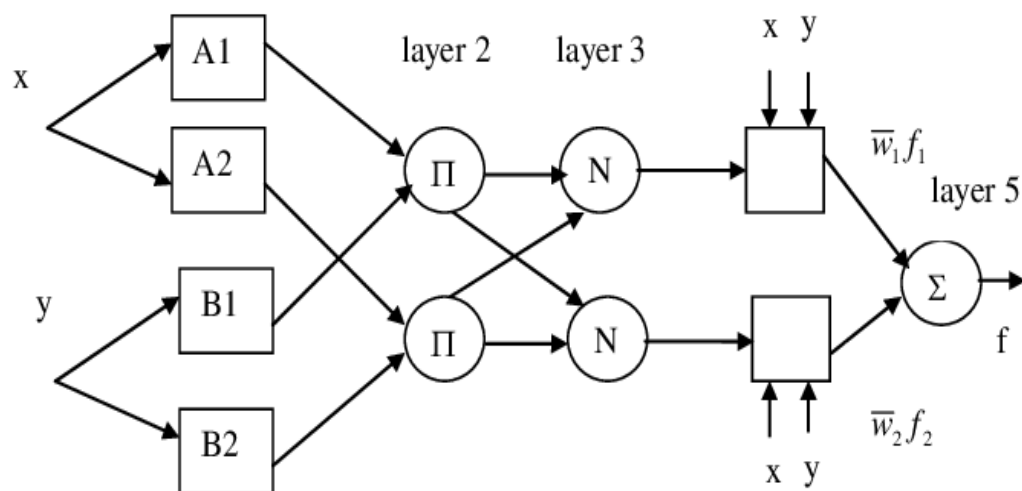


Figure (9): The ANFIS general Architecture

### 8-OpenCV:

which is one of the widely used and its an open source so we are going put a light on it.

OpenCV (Open-Source Computer Vision Library) is a library of programming functions mainly aimed at real-time computer vision. Originally developed by Intel, it was later supported by Willow Garage then Tires the library is cross-platform and free for use under the open-source Apache 2 License. Starting with 2011, OpenCV features GPU acceleration for real-time operation..... [20] OpenCV is written in C++ and its primary interface is in C++, but it still retains a less comprehensive though extensive older C interface. All of the new developments and algorithms appear in the C++ interface. There are bindings in Python, Java and MATLAB/OCTAVE. The API for these interfaces can be found in the online documentation. Wrappers in several programming languages have been developed to

## Chapitre2: face recognition system

encourage adoption by a wider audience. In version 3.4, JavaScript bindings for a selected subset of OpenCV functions was released as OpenCV.js, to be used for web platforms... [21]

-applications using OpenCV, some of them are listed below:

Automated inspection and surveillance.

number of people – count (foot traffic in a mall...).

Vehicle counting on highways along with their speeds

Interactive art installations.

Anatoly (defect) detection in the manufacturing process (the odd defective products).

Street view image stitching.

Video/image search and retrieval.

Robot and driver-less car navigation and control.

object recognition.

Medical image analysis.

Movies – 3D structure from motion.

TV Channels advertisement recognition. ....[22]

And the most important application is the one that this project going to be based on which is security camera based on face recognition.

-Computer Vision overlaps significantly with the following fields:

**Image Processing:** It focuses on image manipulation. **Pattern Recognition:** It explains various techniques to classify patterns.

**Photogrammetry:** It is concerned with obtaining accurate measurements from images.

### -Computer Vision Vs Image Processing:

Image processing deals with image-to-image transformation. The input and output of image processing are both images.

Computer vision is the construction of explicit, meaningful descriptions of physical objects from their image. The output of computer vision is a description or an interpretation of structures in 3D scene.

### -Features of OpenCV Library

Read and write images.

Capture and save videos.

Process images (filter, transform).

Perform feature detection.

Detect specific objects such as faces, eyes, cars, in the videos or images.

Analyze the video, i.e., estimate the motion in it, subtract the background, and track objects in it.

### -OpenCV Library Modules

Following are the main library modules of the OpenCV library.

**Core Functionality:** This module covers the basic data structures such as Scalar, Point, Range, etc., that are used to build OpenCV applications. In addition to these, it also includes the multidimensional array Mat, which is used to store the images. In the Java library of OpenCV, this module is included as a package with the name `org.opencv.core`.

**Image Processing:** This module covers various image processing operations such as image filtering, geometrical image transformations, color space conversion, histograms, etc. In the Java library of OpenCV, this module is included as a package with the name `org.opencv.imgproc`.

**Video:** This module covers the video analysis concepts such as motion estimation, background subtraction, and object tracking. In the Java library of OpenCV, this module is included as a package with the name `org.open cv. video`.

**Video I/O:** This module explains the video capturing and video codecs using OpenCV library. In the Java library of OpenCV, this module is included as a package with the name `org.open cv. video`.

**calib3d:** This module includes algorithms regarding basic multiple-view geometry algorithms, single and stereo camera calibration, object pose estimation, stereo correspondence and elements of 3D reconstruction. In the Java library of OpenCV, this module is included as a package with the name `org.opencv.calib3d`.

**features2d:** This module includes the concepts of feature detection and description. In the Java library of OpenCV, this module is included as a package with the name `org.opencv.features2d`.

**Objdetect:** This module includes the detection of objects and instances of the predefined classes such as faces, eyes, mugs, people, cars, etc. In the Java library of OpenCV, this module is included as a package with the name `org.opencv.objdetect`.

**Highgui:** This is an easy-to-use interface with simple UI capabilities. In the Java library of OpenCV, the features of this module is included in two different packages namely, `org.opencv.imgcodecs` and `org.opencv.videoio`. [23]

-And there is another library that going to be used specifically in this project later on like `dlib`.

### 9-LBPH algorithm (Local Binary Pattern Histogram) :

#### Introduction:

LBPH (Local Binary Pattern Histogram) is a Face-Recognition algorithm it is used to recognize the face of a person. It is known for its performance and how it is able to recognize the face of a person from both front face and side face.

Working of the LBPH algorithm:

The LBPH algorithm typically makes use of 4 parameters:

**Radius:** The distance of the circular local binary pattern from the center pixel to its circumference and usually takes a value of 1.

**Neighbors:** The number of data points within a circular local binary pattern. Usually, the value of 8.

**Grid X:** The number of cells in the horizontal plane, is usually a value of 8.

**Grid Y:** The number of cells in the vertical plane, is usually a value of 8.

Given the above-mentioned parameters, LBPH works as follows;

A data set is created by taking images with a camera or taking images that are saved, and then provisioning a unique identifier or name of the person in the image and then adding the images to a database. It is recommended to take many samples from a single individual. A portion of the data set is used for the training of the algorithm, while the rest is used for testing.

Using a circular neighborhood concept (which takes non-integer pixel points around a selected area), the number of appearances of LBP codes in the image is put together to form a histogram. The classification is then carried out through the calculation of the basic similarities of the histograms under comparison.

This histogram contains a description of an individual at three different levels: at a pixel-level, labels are combined in a small area to create a regional level, the regional histograms in combination build a general description of the person.

### **modes of operation of face recognition:**

The face recognition algorithm generally operates in one of two modes:

**Authentication of a facial image:** This mode does facial recognition by a 1x1 comparison. The comparison is done between an input image and a specific image within the database. In many cases, this is the face that requires authentication at the time of this mode of facial recognition.

**Face recognition:** in this mode, it is a 1xN, a comparison of the input face image with all the pictures that have been saved in the database to output the images of the user which conforms to the input face image.

### **Computational steps:**

**The application of the LBP operation:** is the first step of the computational steps. Here, an intermediate image has been created to better represent the original image

through a sliding window concept, taking into account two parameters: the neighbor and the radius. New values are created in the form of binary by comparing the 8 neighbor values to the threshold value.

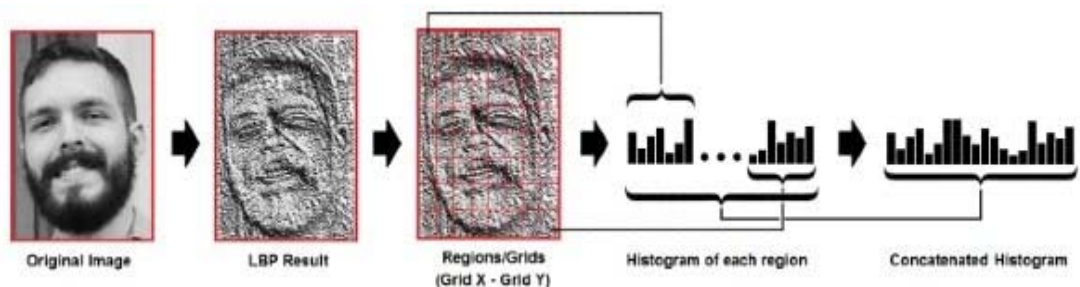
For each neighbor value greater than the threshold value, the value is set to 1 and 0 for every neighbor value less than the threshold value. This forms a matrix of binary numbers excluding the threshold. A central value of the matrix is created by the conversion of the binary number to a decimal value which corresponds to the pixels of the original image. For a better representation of the characteristics of the original image.

The following image illustrates the above conversions:

Performing LBP operation on an image

-To Extract Histograms: The image obtained in step is divided into multiple grids, with the help of the Grid parameters X and Y. This image is in grayscale, each of the histograms of each of the grids is to represent the intensity of the occurrences of each pixel. Each histogram is then combined to create a new histogram that represents the attributes of the original image.

The following image illustrates the above extraction:



Figure[10]:image illustrates the above extraction

## II.5 ADVANTAGES AND DISADVANTAGES OF FACE recognition system:

### II.5 .1 ADVANTAGES OF FACE RECOGNITION SYSTEM:

Better security. Face detection augments surveillance tactics and forms the basis of the identification process of terrorists and criminals;Easy to integrate. Most face detection solutions are compatible with security software;Automated identification.

Face detection lets facial identification be automated, thus increasing efficiency alongside a heightened rate of accuracy.

### **II.5 .2DISADVANTAGES OF FACE RECOGNITION SYSTEM:**

huge storage requirements. Machine learning technology requires powerful data storage.

Detection can be vulnerable. We've outlined the way in which facial detection can be thrown off.

Potential privacy issues. There is disagreement on whether face detection is compatible with human privacy rights.

### **II.6 Cameras:**

Beside the importance of the software which revels in many types of algorithms that help in put the whole idea of face recognition and a security system based on it as a whole on work, there is the equipment that appear mainly as cameras which we are going to have a brief overview at.

**II.6 .1.General definition of camera:** a camera is an optical instrument that captures a visual image. At a basic level, cameras consist of sealed boxes with a small hole that allows light through to capture an image on a light-sensitive surface.

Cameras have various mechanisms to control how the light falls onto the light-sensitive surface. Lenses focus the light entering the camera. The aperture can be narrowed or widened.

A shutter mechanism determines the amount of time the photosensitive surface is exposed to light.....[24]

**II.6.2.Types of cameras:** there are a lot of cameras that provide a lot of features, but when it comes to face recognition only smart cameras will be part of the system and for the record there is not a lot of types

1-2D Camera, which creates a flat image of a face, and maps 'nodal points' (size/shape of eyes, nose, cheekbones, etc.). The system then calculates the nodes' relative position and converts the data into a numerical code. The recognition algorithms search a stored database of faces for a match. works well in stable, well-lit conditions such as passport control. But it is

## Chapitre2: face recognition system

less effective in darker spaces and cannot deliver good results when the subjects move around. It is easy to spoof with a photograph.....[25]

2- 3D camera is an imaging device that enables the perception of depth in images to replicate three dimensions as experienced through human binocular vision. Some 3D cameras use two or more lenses to record multiple points of view, while others use a single lens that shifts its position.....[26]



Figure 11 : cameras



## **Chapitre III : application and results**

### *III.introduction*

### *III.2 Components Required*

### *III.3 Circuit Diagram*

### *III.4 Installing OpenCV in Raspberry Pi 3*

### *III.5 coding for Face Recognition Door Lock*

### *III.6 Testing the Raspberry Pi Face Recognition Door Lock*

### *III.7 The complete code*

### Chapter III: application and results

#### III.1 Introduction:

Face Recognition Door Lock System using Raspberry Pi is an advanced feature in digital locks where people can easily unlock the door using their faces. All you need to do is position your face in front of the lock, following which the camera scans it to check if it matches correctly with the pre-stored faceprints and then unlocks the door for you. This project consists of three phases that are important in face recognition logic which are:

-Data Gathering

-Training the Recognizer

-Face Recognition

And in order to make everything clear we have to put a little of explanation on each phase that need to be used. And we have to start with the first phase, which is Data Gathering which with we will collect the face samples that are authorized to open the lock. And In the second phase, we will train the Recognizer for these face samples that we had collected in previous step, and in the last phase would be trainer data and will be used to recognize the faces. If raspberry pi recognizes a face, it will open the door lock otherwise the door still locked.

#### III.2Components Required:

Raspberry Pi 3 (any version)

Solenoid Lock

Relay Module

Jumper Wires

Raspberry Pi camera

External DC power source

#### III.3 Circuit Diagram:

Circuit diagram of the project.

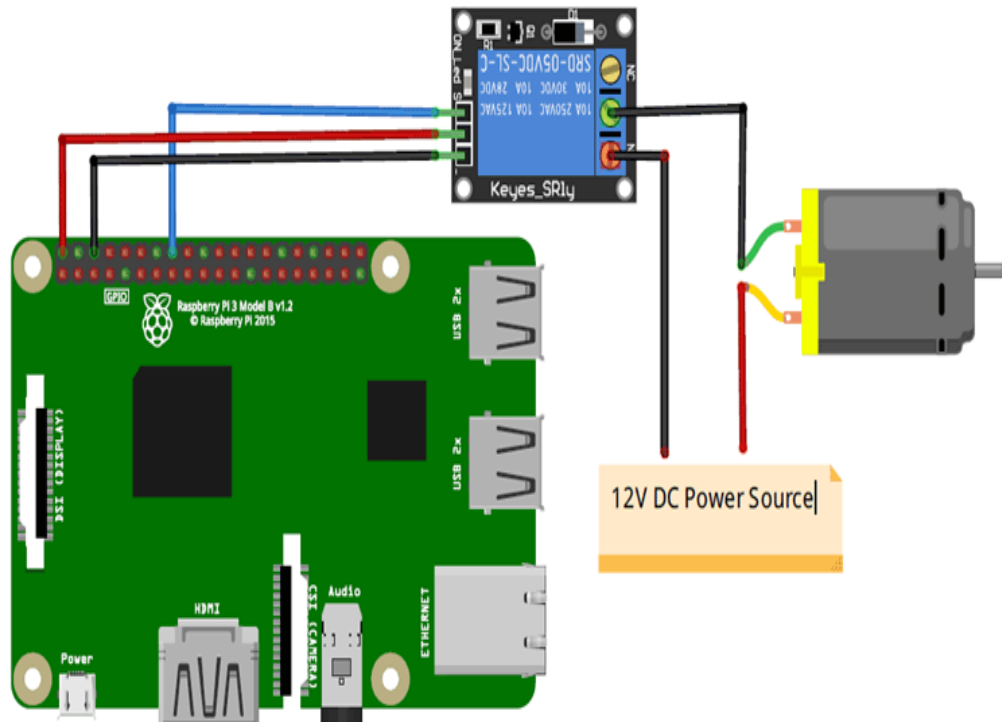


Figure 12 : circuit diagram

Raspberry Pi and Solenoid Lock are connected through the relay module. Solenoid lock requires 9 to 12V which the Raspberry pi cannot provide because its limit is only 5V. Due to this problem thought that we have to use a 12V adapter in order to power the Solenoid Lock and provide the voltage that needed to make the system function. VCC and GND pin of the relay module is connected to 5V and ground of Raspberry Pi. The input pin of the relay is connected to GPIO20 of Raspberry Pi.

The positive pin of Solenoid lock is connected to the positive rail of the 12V adapter, while the negative pin of Solenoid Lock is connected to COM of Relay. Connect the NO pin of the relay to Negative of 12V adapter

### III.4 Installing OpenCV in Raspberry Pi 3:

#### Step 1: Set Up Your Raspberry Pi

first thing first you should make sure your Raspberry Pi is using the full SD card. And here is the work.

## Chapitre 3 : application and results

you need to get in your device which is the pi that you use by using the: `sudo raspi-config` and then you have to go to choice number 7 that is advanced options configure advanced setting

```
sudo raspi-config
```

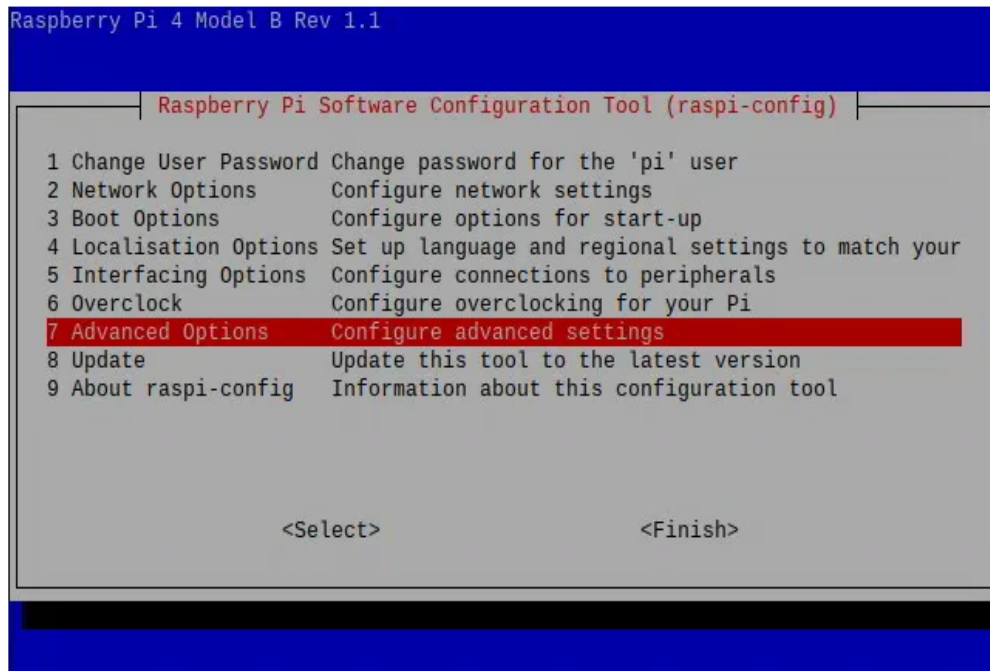
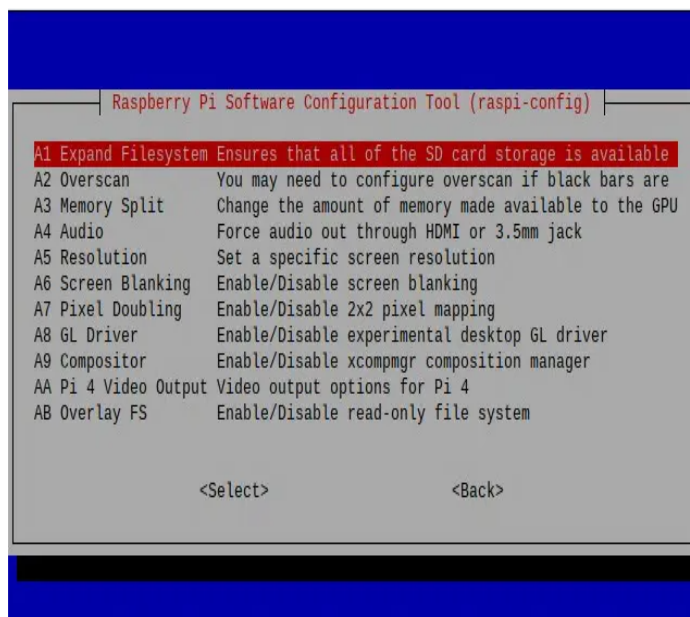


Figure 13: Raspberry Pi configuration

And after that you got to pick A1 expand filesystem ensures that all of the SD card storage is available



## Chapitre 3 : application and results

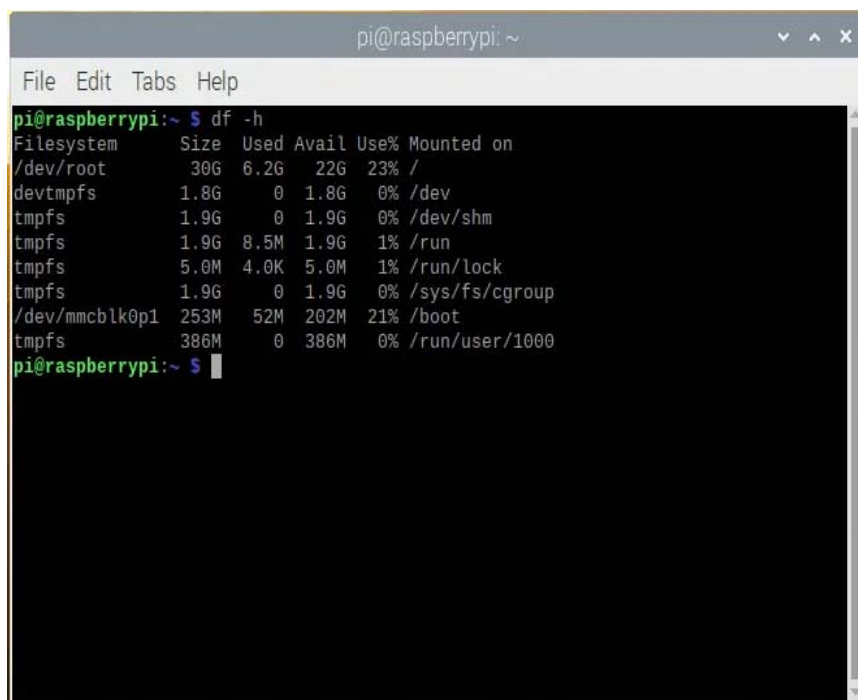
Figure 14: Raspberry Pi configuration tool

-After that you have to reboot by using: `sudo reboot`

```
sudo reboot
```

-and if we want to check if got the job done and we cleared the space we can use: `df -h`

```
df -h
```



```
pi@raspberrypi: ~  
File Edit Tabs Help  
pi@raspberrypi:~$ df -h  
Filesystem      Size  Used Avail Use% Mounted on  
/dev/root        30G   6.2G   22G   23% /  
devtmpfs         1.8G     0   1.8G    0% /dev  
tmpfs            1.9G     0   1.9G    0% /dev/shm  
tmpfs            1.9G   8.5M   1.9G    1% /run  
tmpfs            5.0M   4.0K   5.0M    1% /run/lock  
tmpfs            1.9G     0   1.9G    0% /sys/fs/cgroup  
/dev/mmcblk0p1   253M   52M  202M   21% /boot  
tmpfs            386M     0   386M    0% /run/user/1000  
pi@raspberrypi:~$
```

-then the next major thing that needs to be done is update the system and to do so we have to use this:

```
sudo apt-get update && sudo apt-get upgrade
```

-Then use the following commands to install the required dependencies for installing OpenCV on your Raspberry Pi:

```
sudo apt-get install libhdf5-dev -y
```

```
sudo apt-get install libhdf5-serial-dev -y
```

```
sudo apt-get install libatlas-base-dev -y
```

```
sudo apt-get install libjasper-dev -y
```

## Chapitre 3 : application and results

```
sudo apt-get install libqtgui4 -y
```

```
sudo apt-get install libqt4-test -y
```

-After that, use the below command to install the OpenCV on your Raspberry Pi.

```
pip3 install opencv-contrib-python==4.1.0.25
```

-and even before start thinking about programming, we need to install some important packages:

Installing dlib: dlib is the modern toolkit that contains Machine Learning algorithms and tools for real-world problems. Dlib is an open source suite of applications and libraries written in C++ under a permissive Boost license. Dlib offers a wide range of functionality across a number of machine learning sectors, including classification and regression, numerical algorithms such as quadratic program solvers, an array of image processing tools, and diverse networking functionality, among many other facets.. Use the below command to install the dlib.

```
pip3 install dlib
```

Installing face\_recognition module: This library is used to recognize and manipulate faces from Python through the command line and it is a module. It returns a 2d array of bounding boxes of human faces in an image using the CNN face detector. If you are using a GPU, this can give you much faster results since the GPU can process batches of images at once. If you aren't using a GPU, you don't need this function.. Use the below command to install the face recognition library.

```
Pip3 install face_recognition
```

Installing imutils: imutils is used to make essential image processing functions such as translation, rotation, resizing, skeletonization, and displaying Matplotlib images easier with OpenCV. Use the below command to install the imutils:

```
pip3 install imutils
```

Installing pillow: Pillow is Python Imaging Library is a free and open-source additional library for the Python programming language that adds support for opening, manipulate, and save images in a different format. Use the below command to install pillow:

```
pip3 install pillow
```

### **III.5 coding for Face Recognition Door Lock:**

As we mentioned before, we are going to build this project in three-phase. The first phase is data gathering and the second is training the Recognizer, and the third is recognizing the faces.

The first thing we start with is Data Gathering:

-create a Dataset to store the faces. These faces will be stored with different IDs. For that, first, create a project directory where all the project data will be saved

```
yeah FaceRecognition
```

along with the three-python program and Dataset, this directory also has a Facial Classifier file.

-And then inside the FaceRecognitionProject directory, create a new subdirectory names Dataset to store the face samples.

```
yeah Dataset
```

-we need to open a Nano editor file in FaceRecognitionProject directory and put the data gathering coding in.

```
sudo nano dataset.py
```

1) we want to explain Data Gathering program:

-Initialize the face detector. The facial classifier file is used with a face detector.

```
face_detector = cv2.CascadeClassifier('haarcascade_frontalface_default.xml')
```

## Chapitre 3 : application and results

-Now provide a user input command so that the user can enter the numeric face id before gathering the data.

```
face_id = input('\n enter user id end press ENTER ==> ')
```

-Inside the while loop, use the detector to extract the faces.

```
ret, img = cam.read()

img = cv2.flip(img, -1) # flip video image vertically

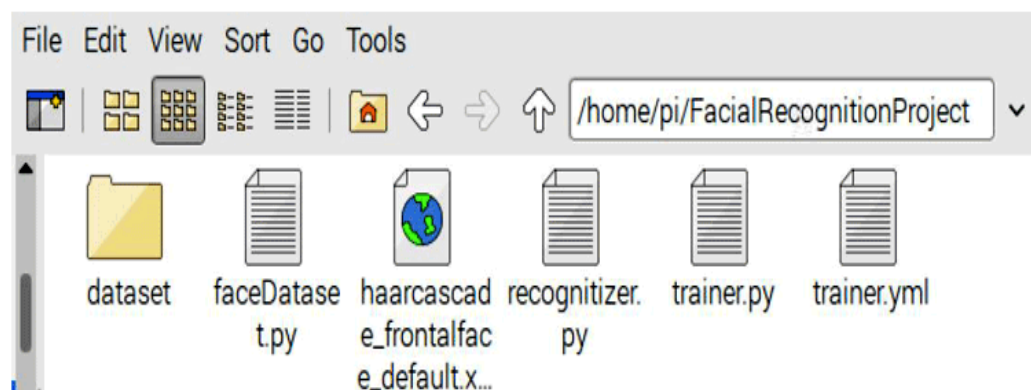
gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)

faces = face_detector.detectMultiScale(gray, 1.3, 5)
```

-After that, save each one of the captured frames, save it as a file on a "dataset" directory with the person id:

```
cv2.imwrite("dataset/User." + str(face_id) + '.' + str(count) + ".jpg",
gray[y:y+h,x:x+w])
```

-Run the python coding and enter the face id. When it detects a face, it starts capturing the samples. And then samples will be saved inside the Dataset directory.



### Training the Recognizer:

After collecting the face samples, we have to train the Recognizer for these samples so that it can know the faces accurately.



## Chapitre 3 : application and results

Next step is Opening a Nano editor file inside the Face Recognition directory and we have a code and more likely under the name trainer; exactly trainer.py And here is a little of explanation of the code that called trainer:

-Start the code by importing all the required library files.

```
import cv2  
  
import numpy as np  
  
from PIL import Image  
  
import os
```

-After that, enter the path where you saved the face samples.

```
path = 'dataset'
```

-Next up, we have used the haarcascade\_frontalface\_default.xml facial classifier file to detect the faces in sample images. Then use the recognizer variable to create an LBPH (Local Binary Pattern Histogram) Face Recognizer.

```
detector = cv2.CascadeClassifier("haarcascade_frontalface_default.xml");  
  
recognizer = cv2.face.LBPHFaceRecognizer_create()
```

-Now we got into the face samples directory using the path that been initialized earlier.

```
imagePaths = [os.path.join(path,f) for f in os.listdir(path)]
```

-After that, create two lists for storing face pics and theIDs.

```
facepics=[]  
  
theIDs = []
```

- then we Converted the image samples into grayscale. After that, we did convert the PIL image into a numpy image.

```
PIL_img = Image.open(imagePath).convert('L') # convert it to grayscale
```

## Chapitre 3 : application and results

```
img_numpy = np.array(PIL_img, 'uint8')
```

-Sample in the Dataset directory is saved like this: User.Id.SampleNumber. So, to get the ID, we will divide the image path. By dividing the image path, we will get a User ID, and sample number both.

```
id = int(os.path.split(imagePath)[-1].split(".")[1])
```

-after that we called the Faces and theIDs list and feed them into trainer file.

```
faces,theids = getImagesAndLabels(path)
recognizer.train(faces, np.array(theids))
```

and with doing that we have finished the second part of the three basic steps.

Recognizer:

Now we get to the final step of our project, we will use face recognition technology in order to recognize faces from the live video feed. Once raspberry pi recognizes any saved face that he had, automatically it will make the relay module high to open the solenoid lock which this action is the main thing.

And we can say that This program is kind of similar to the trainer program, that they both use the same library files and also the classifier file.

-After that, use an array to add the name for each face id.

```
names = ['None', 'taki', 'naoufe']
```

-the video feed from the raspberry pi camera in 640x480 resolution. and because in using one camera I put zero and in case you are using more than one camera, then replace zero with one in `cam = cv2.VideoCapture(0)` function.

```
cam = cv2.VideoCapture(0)
cam.set(3, 640) # set video width
cam.set(4, 480) # set video height
```

## Chapitre 3 : application and results

-After that, it comes on of the most important steps that we have to make sure that we have executed it perfectly which is inside the while loop, we did break the video into images and then convert it to grayscale.

```
ret, img =cam.read()

img = cv2.flip(img, -1) # Flip vertically

gray = cv2.cvtColor(img,cv2.COLOR_BGR2GRAY)
```

-another important Use recognizer.predict function to check how much the face matches with the samples.

```
cv2.rectangle(img, (x,y), (x+w,y+h), (0,255,0), 2)

id, confidence = recognizer.predict(gray[y:y+h,x:x+w])
```

then we putted the conditions that we want in order the system works. If confidence is closer to 100, then open the lock. 0 means the not a perfect match.

```
if (confidence <= 100):

    id = names[id]

    confidence = " {100}%".format(round(100 - confidence))

    GPIO.output (relay, 1)
```

### III.6 Testing the Raspberry Pi Face Recognition Door Lock:

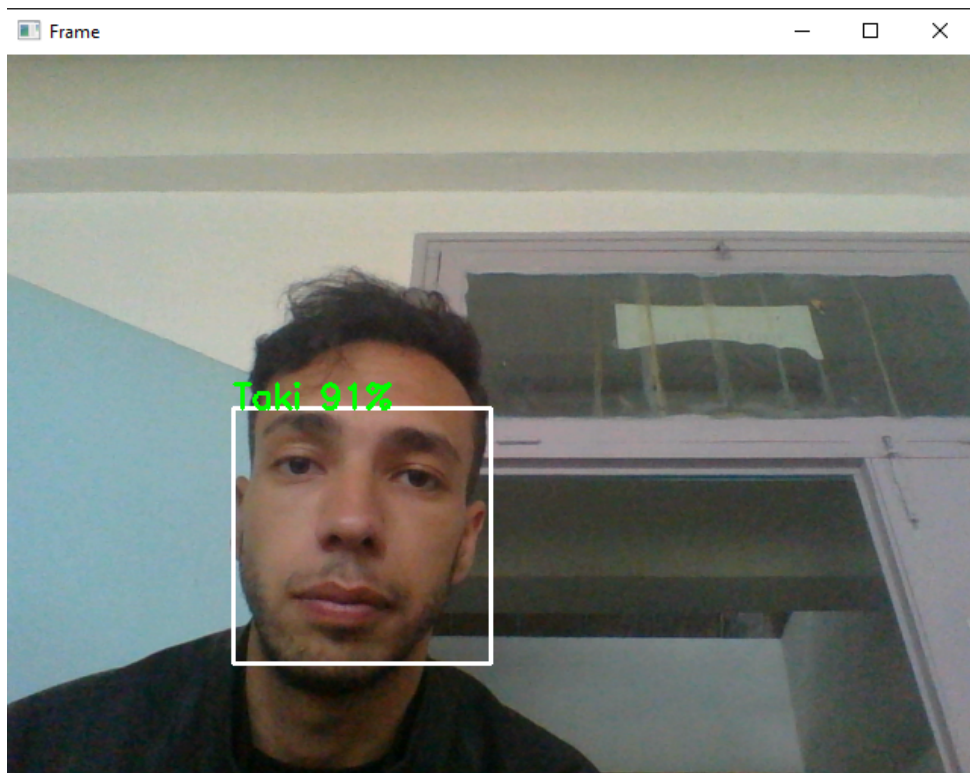
here we are in the last part of this project which is testing the whole work that been putted on it and to do, so we need either an external monitor or any virtual monitor like VNC viewer to execute the codes. As a first step onto executing the work is Runing the dataset program to collect the face samples. When you run the program, a window will show-up. In that window we did enter the ID number and press Enter. After that, there is another window will pop-up just to take the face samples and, in this step, we will use the computer camera. After this we did run the trainer program. Upon a successful execution, it will

### Chapitre 3 : application and results

generate a trainer.yml file into our project directory. This file is a major key and it will be used by Recognizer to recognize the face.

Now in this step, we do run the recognizer program. If a face got recognized in the video feed, you will find a box around it with the name of the person if he was known, or the term **unknown** above the person that was not recognized and then we can say that the program is correct.

-And this is the known face:



And the highest accuracy that we had in our tests was 95% for the known face.

-This is the example of the unknown face :

### Chapitre 3 : application and results



-the highest accuracy that we got when the face was unknown was 96% comparing the the data base that we have.

In the last step the system should get to his final action that contain the lock door which going to interact with the faces on the camera if the person was known then the lock will get an \*1\* which will lead to opening it and if the opposite the lock will not open and, because of the leak of the tools that needed to put the work to a live practice and show you the action in reality we could not make this move.

*important information:* you can put database as much as the memory of the electronic card that you use can contain which mean that the system is flexible when it comes to the number of people whom can be engaged in the system and their faces will be known.

*stuff that can be added to the system in the future:* in order to improve the function of the system and make it work much better the people can add a lot to the idea especially they can add a beneficial feature like connect the whole system to the internet which make it considered as an internet of things. they can make system send a picture of the person who was not recognized by the system as an email to the user.

and to expand the main idea of a security system based on face recognition and put it in a big project they can use it to be part of a smart city which all the houses of it will have that

system in their doors and each system of the houses linked to a main data base center in police station and anytime in any house an unknown person try to get in the house it will send a picture of him to the police station so they can deal with him faster before bad things happen.

### III.7 The complete code:

```
import cv2
import so
cam = cv2.VideoCapture(0)
cam.set(3, 640) # set video width
cam.set(4, 480) # set video height
face_detector = cv2.CascadeClassifier('haarcascade_frontalface_default.xml')

# For each person, enter one numeric face id
face_id = input("\n enter user id end press <return> ==> ")
print("\n [INFO] Initializing face capture. Look the camera and wait ...")

# Initialize individual sampling face count
count = 0
while(True):
    ret, img = cam.read()
    img = cv2.flip(img, -1) # flip video image vertically
    gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
    faces = face_detector.detectMultiScale(gray, 1.3, 5)
    for (x,y,w,h) in faces:
        cv2.rectangle(img, (x,y), (x+w,y+h), (255,0,0), 2)
        count += 1

    # Save the captured image into the datasets folder
    cv2.imwrite("dataset/User." + str(face_id) + '.' + str(count) + ".jpg", gray[y:y+h,x:x+w])
    cv2.imshow('image', img)
    k = cv2.waitKey(100) & 0xff # Press 'ESC' for exiting video
    if k == 27:
```

```
        break
    elif count >= 30: # Take 30 face pics and stop video
        break

# Do a bit of cleanup
print("\n [INFO] Exiting Program and cleanup stuff")
cam.release()
cv2.destroyAllWindows()

import cv2
import numpy as np
from PIL import Image
import os

# Path for face image database
path = 'dataset'
recognizer = cv2.face.LBPHFaceRecognizer_create()
detector = cv2.CascadeClassifier("haarcascade_frontalface_default.xml");

# function to get the images and label data
def getImagesAndLabels(path):
    imagePath = [os.path.join(path,f) for f in os.listdir(path)]
    facepics=[]
    theids = []
    for imagePath in imagePath:
        PIL_img = Image.open(imagePath).convert('L') # convert it to grayscale
        img_numpy = np.array(PIL_img,'uint8')
        id = int(os.path.split(imagePath)[-1].split(".")[1])
        faces = detector.detectMultiScale(img_numpy)
        for (x,y,w,h) in faces:
            facepics.append(img_numpy[y:y+h,x:x+w])
            theids.append(id)
    return facepics,theids
```

## Chapitre 3 : application and results

```
print ("\n [INFO] Training faces. It will take a few seconds. Wait ...")
faces,theids = getImagesAndLabels(path)
recognizer.train(faces, np.array(theids))

# Save the model into trainer/trainer.yml
recognizer.write('trainer.yml') # recognizer.save() worked on Mac, but not on Pi

# Print the numer of faces trained and end program
print("\n [INFO] {0} faces trained. Exiting Program".format(len(np.unique(theids))))

import cv2
import numpy as np
import os
import RPi.GPIO as GPIO
import time
relay = 20
GPIO.setwarnings(False)
GPIO.setmode(GPIO.BCM)
GPIO.setup(relay, GPIO.OUT)
GPIO.output(relay ,1)
recognizer = cv2.face.LBPHFaceRecognizer_create()
recognizer.read('trainer.yml')
cascadePath = "haarcascade_frontalface_default.xml"
faceCascade = cv2.CascadeClassifier(cascadePath);
font = cv2.FONT_HERSHEY_SIMPLEX

#iniciate id counter
id = 0

# names related to ids: example ==> Marcelo: id=1, etc
names = ['unknown', 'taki']

# Initialize and start realtime video capture
```



```
cam = cv2.VideoCapture(0)
cam.set(3, 640) # set video width
cam.set(4, 480) # set video height

# Define min window size to be recognized as a face
minW = 0.1*cam.get(3)
minH = 0.1*cam.get(4)
while True:
    ret, img = cam.read()
    img = cv2.flip(img, -1) # Flip vertically
    gray = cv2.cvtColor(img, cv2.COLOR_BGR2GRAY)
    faces = faceCascade.detectMultiScale(
        gray,
        scaleFactor = 1.2,
        minNeighbors = 5,
        minSize = (int(minW), int(minH)),
    )
    for(x,y,w,h) in faces:
        cv2.rectangle(img, (x,y), (x+w,y+h), (0,255,0), 2)
        id, confidence = recognizer.predict(gray[y:y+h,x:x+w])

        # Check if confidence is less than 100 ==> "0" is perfect match
        if (confidence < 100):
            id = names[id]
            confidence = " {0}%".format(round(100 - confidence))
            GPIO.output(relay, 0)
            print("Opening Lock")
#         time.sleep(1)
#         GPIO.output(relay, 1)
        else:
            id = "unknown"
            confidence = " {0}%".format(round(100 - confidence))
            GPIO.output(relay, 1)
```

## Chapitre 3 : application and results

```
cv2.putText(img, str(id), (x+5,y-5), font, 1, (255,255,255), 2)
cv2.putText(img, str(confidence), (x+5,y+h-5), font, 1, (255,255,0), 1)
cv2.imshow('camera',img)
k = cv2.waitKey(10) & 0xff # Press 'ESC' for exiting video
if k == 27:
    break
# Do a bit of cleanup
print("\n [INFO] Exiting Program and cleanup stuff")
cam.release()
cv2.destroyAllWindows()
```

### Conclusion:

he whole system is working perfectly despite the fact that we couldn't do a realisation for the action of the lock open for the known person and reject the unknown. as we saw that the system detected the face of the person who was known for it and have a data about him already, and in the opposit it did not recognized the person whom the system do not have a data that difine him and make him known for the system.and also can put data as much as the memory of the electronic card that you work with can contain therefor we can put alot of faces that the system could interact with.

Prespective:

- ✂ first prespective is that we can add a beneficial feature like connect the whole system to the internet which make it considered as an internet of things. they can make system send a picture of the person who was not recognized by the system as an email to the user.
- ✂ Second prspective is that we can put the system in a big project and make the data base huge which it can be part of a smart city to increase the efficiency of the security.

### **General Conclusion:**

human seeking safety and having that instinct of trying their best to secure themselves over the ages lead up to develop the technology that engage in every part of people life in general and specially the parts that linked to security which manifest itself at many types of securities and especially in the last several years been focused at face recognition technology to develop and improve its efficiency and accuracy of the recognition because it allows only the chosen people and whom putted their faces in the database that used to pass by the security system and that gives the users the safety that they need throughout their daily life. and by combining the desire of security that human have and the new technology we will end up with our project idea which is security system based on face recognition and it require a simple hardware and software.

I can say that our project fulfilled human desire of security efficiently and in a fashionable way because it bringed everything that needed to the table together in an harmonical way.

## BIBLIOGRAPHIE:

- [1] <https://en.wikipedia.org/wiki/Security> \_ wikipedia article \_ introduction for security \_
- [2] <https://www.vodafone.com/business/news-and-insights/blog/gigabit-thinking/a-brief-history-of-security> \_ article \_ by Simon Fenn
- [3] <https://twentyfirstsecurity.com.au/blog/a-brief-history-of-security-through-the-ages/> \_artical \_ security history
- [4] <https://sonitrolsecurity.com/how-the-archaeological-periods-relate-to-security/> \_article \_ security history
- [5] <https://scgroup.global/blog/9-reasons-why-electronic-security-systems-important-business/> \_article \_ significance of security system
- [6] <https://www.openpath.com/physical-security-guide> \_article \_physical security systems
- [7] <https://theconstructor.org/building/building-security-control/6973/> \_article \_ physical security systems applications
- [8] <https://www.itgovernance.co.uk/what-is-cybersecurity> \_article \_ cyber security system
- [9] <https://www.kaspersky.com/resource-center/definitions/what-is-cyber-security>
- [10] artical Published in: 2018 International Conference on Smart City and Emerging Technology (ICSCET) by Prashanth Balraj Balla / K. T. Jadhao \_ introduction on Facial Recognition Security System
- [11] [https://en.wikipedia.org/wiki/Facial\\_recognition\\_system](https://en.wikipedia.org/wiki/Facial_recognition_system) article on facial recognition systems
- [12] face recognition using deep neural networks by dubois , artoime- 2018
- [13] [https://en.wikipedia.org/wiki/Facial\\_recognition\\_system](https://en.wikipedia.org/wiki/Facial_recognition_system) \_article \_ History and elevation of face recognition system

### Chapitre 3 : application and results

- [14] <https://www.nytimes.com/wirecutter/blog/how-facial-recognition-works/> \_article\_ by Thorin Klosowski PUBLISHED JULY 15, 2020 about General understanding of facial recognition software works
- [15] <https://www.analyticssteps.com/blogs/top-deep-learning-algorithms> \_article\_ by Ayush Singh Rawat PUBLISHED Mar 04, 2021 about Machine learning
- [16] <https://machinelearningmastery.com/what-is-deep-learning/> article about Deep Learning by Jason Brownlee on August 16, 2019
- [17] <https://data-flair.training/blogs/artificial-neural-networks-for-machine-learning/> \_article\_ about Artificial Neural Networks
- [18] <https://recfaces.com/articles/facial-recognition-algorithms> \_article\_ PUBLISHED 25 MARCH 2021
- [19] <https://iq.opengenus.org/face-recognition-using-fisherfaces/> \_article\_ about Fisher Faces Process
- [20] <https://en.wikipedia.org/wiki/OpenCV> \_article\_ about OpenCV
- [21] <https://en.wikipedia.org/wiki/OpenCV> programming language \_article\_ about OpenCV
- [22] <https://www.geeksforgeeks.org/opencv-overview/> Article about applications using OpenCV
- [23] [https://www.tutorialspoint.com/opencv/opencv\\_overview.htm](https://www.tutorialspoint.com/opencv/opencv_overview.htm) Article Contributed By : ramswarup\_kulhary in 05 Aug, 2021 about opencv librarys
- [24] <https://en.wikipedia.org/wiki/Camera> Article about camera
- [25] [www.thalesgroup.com/en/markets/digital-identitysecurity/government/inspired/history-of-facial-recognition](http://www.thalesgroup.com/en/markets/digital-identitysecurity/government/inspired/history-of-facial-recognition) Article about 2D Camera
- [26] [www.techtarget.com/whatis/definition/3D-camer](http://www.techtarget.com/whatis/definition/3D-camer) Article about 3D Camera