



Mohamed Khider University of Biskra
Faculty of Science and Technology
Electrical Engineering Department

MASTER DISSERTATION

Science and Technology
Electrical Engineering
Automatic

Ref.: Enter the document reference

Presented and supported by:
HIOUNI Islam

The:

GUI MATLAB For Biometric Recognition

Jury:

Dr. MECHGOUG Raihane	MCA	University Of Biskra	President
Dr. MEGHERBI Hassina	MCA	University Of Biskra	Examiner
Dr. ZITOUNI Athmane	MCA	University Of Biskra	Protractor

University Year: 2021 - 2022



Mohamed Khider University of Biskra
Faculty of Science and Technology
Electrical Engineering Department

MASTER DISSERTATION

Science and Technology
Electrical Engineering
Automatic

Ref.: Enter the document reference

GUI MATLAB For Biometric Recognition

The:

Presented By:

HIOUNI Islam

Favorable opinion of the supervisor:

Dr. ZITOUNI Athmane

Signature Favorable opinion of the President of the Jury

Dr. MECHGOUG Raihane

Stamp and signature

Abstract:

A facial recognition framework is one type of biometrics technology that could be a computer application able of distinguishing or confirming an individual from a computerized picture or a video outline from a video source. The work represented in this manuscript is to consider and develop a face recognition system by the clean faces of strategy, we used the method that allows us to achieve our goal in this project with MATLAB application.

Keywords: Facial recognition, biometrics technology, GUI, MATLAB.

ملخص:

يمكن أن يكون إطار عمل التعرف على الوجه أحد أنواع تقنيات القياسات الحيوية عبارة عن تطبيق كمبيوتر قادر على تمييز أو تأكيد شخص ما من صورة محوسبة أو مخطط فيديو من مصدر فيديو. العمل المعروف في هذا المشروع هو النظر في نظام الإدراك البشري وتحقيقه من خلال الوجوه النظيفة للاستراتيجية التي استخدمناها بطريقة تسمح بتحقيق هدفنا في هذا المشروع مع استخدام برنامج .MATLAB

الكلمات المفتاحية: التعرف على الوجه، تكنولوجيا القياسات الحيوية، GUI، MATLAB

Résumé:

Un cadre de reconnaissance faciale, l'un des types de technologie biométrique, pourrait être une application informatique capable de distinguer ou de confirmer un individu à partir d'une image informatisée ou d'un contour vidéo à partir d'une source vidéo. Le travail présenté dans cette mémoire consiste à considérer et réaliser un système cognitif humain par les visages propres de la stratégie que nous avons utilisée permet d'atteindre notre objectif dans ce projet.

Mots-clés: La reconnaissance biometrique, technologie biometrique, GUI, MATLAB

DEDICATIONS

At the end of this work, I would like to pay tribute to all those who have given me their encouragement. I dedicate this milestone in my life to:

The memory of my father Hiouni Saddok

-Since my early childhood you have been the best father in the world, a great man with every sense of the term. Today I am here to reap the rewards of 22 years of hard work and diligence, I stand where you always wanted to see me.

Thank you, dad, for what you have always been for me, you wished so much that I achieve this goal. Today my success is yours, today I follow in your footsteps. I like you. God bless your soul.

The dearest being of my life my mother

This work is the fruit of your sacrifices that you have made for my education and my training. All the words in the world cannot express the immense love that I have for you, nor the deep gratitude that I show you. It is thanks to you that I am here today.

My beautiful, you have always supported, understood and comforted me. Thank you for being here, May Almighty God keep you and give your health, happiness, and long life.

My dear brothers and sisters

My big brother Salah Eddine and his two children Nibras and Afnane, our little pharmacist Med Wassim, Nassima and his daughter Mélina, Lamia and his son Louai, our dentist Imane, little Ibtihal and my sister-in-law Abir, you are for me brothers, sisters and also friends on whom I can count.

As a testament to the memories of all the times we spent together, I dedicate this work to you.

My woman Ines

My source of hope and motivation, I am proud to have chosen you as the woman of my life.

Your help was the cause that revived me in difficult times, and allowed me to succeed.

My dear friends Wail and Mohammed

In remembrance of our friendship. Thank you for all the moments spent with you.

May God give you all the happiness you deserve.

THANKS

First of all, we would like to thank Allah almighty for giving us the strength to accomplish this modest work.

My most sincere thanks go to anyone who had the kindness and patience to help me in my work with their valuable advice, answers and recommendations.

I would like to thank and express my deep gratitude to the director of the faculty of science and technology, to the head of the electrical engineering department, and all the teachers for their encouragement and valuable advice.

At the same time, I would like to thank my supervisor, for his good supervision and his desire to work in the best conditions with his great experience and his fruitful advice that he never stopped giving me.

My last word goes to all the members of the jury who agreed to evaluate my modest work.

SUMMARY

LIST OF ABBREVIATIONS.....	IV
LIST OF FIGURES & TABLES	V
GENERAL INTRODUCTION	VII
CHAPTER I: BIOMETRIC TECHNOLOGY	1
I.1 INTRODUCTION.....	1
I.2 BIOMETRIC	1
I.2.1 Definition.....	1
I.2.2 Biometric Characteristics	2
I.2.3 The different biometric modalities	3
I.2.3.1 Physiological Biometrics.....	4
I.2.3.1.1 Iris:	4
I.2.3.1.2 Finger Prints	5
I.2.3.1.3 Facial Recognition	6
I.2.3.1.4 Vein Recognition	6
I.2.3.2 Behavioral Biometrics	7
I.2.3.2.1 Keystroke Dynamics.....	7
I.2.3.2.2 Vocal (Speech) Recognition	7
I.2.3.2.3 Signature Dynamics.....	8
I.2.3.3 Biological biometrics	9
I.2.3.3.1 Deoxyribonucleic Acid (DNA).....	9
I.2.3.3.2 Blood	9
I.3 BIOMETRIC SYSTEMS	10
I.3.1 Definition.....	10
I.3.2 Biometric System Modules	11
I.3.3 Performance evaluation of biometric systems	12
I.3.4 Reliability of biometric systems.....	13
I.3.5 Application of Biometrics.....	13
I.4 CONCLUSION	14
CHAPTER II: FACIAL RECOGNITION	15
II.1 INTRODUCTION.....	15

II.2	FACIAL RECOGNITION	15
II.2.1	<i>Definition</i>	15
II.2.2	<i>Facial Recognition Steps</i>	16
II.2.3	<i>Application of facial recognition</i>	17
II.2.4	<i>Examples of facial recognition technology</i>	19
II.3	FACE RECOGNITION METHODS	21
II.3.1	<i>Eigen Face</i>	21
II.3.2	<i>Gabor Wavelet</i>	22
II.3.3	<i>Neural Network (NN)</i>	23
II.3.4	<i>Hidden Markov Model (HMM)</i>	24
II.3.5	<i>Support Vector Machine (SVM)</i>	25
II.4	ADVANTAGES AND DISADVANTAGES OF FACE RECOGNITION.....	26
II.4.1	<i>Advantages</i>	26
II.4.2	<i>Disadvantages</i>	27
II.5	FACIAL RECOGNITION SECURITY - HOW TO PROTECT YOURSELF	28
II.6	CONCLUSION	29
CHAPTER III: FACE DETECTION THE VIOLA-JONES METHOD		30
III.1	INTRODUCTION.....	30
III.2	ALGORITHM	31
III.2.1	<i>Input Image</i>	31
III.2.2	<i>Haar Feature Selection</i>	32
III.2.3	<i>Integral image:</i>	34
III.2.4	<i>Adaptive boosting (Adaboost)</i>	35
III.2.5	<i>Cascading classifiers</i>	36
III.3	CONVOLUTIONAL NEURAL NETWORK (CNN).....	38
III.3.1	<i>Definition</i>	38
III.4	CONCLUSION	38
CHAPTER IV: APPLICATION WITH GUI MATLAB		39
IV.1	INTRODUCTION.....	39
IV.2	WORKING ENVIRONMENT.....	39
IV.3	DEVELOPMENT TOOLS	39
IV.3.1	<i>MATLAB 2020a</i>	39

SUMMARY

IV.3.1.1 General Presentation	39
IV.3.1.2 The Peculiarities of MATLAB	40
IV.3.1.3 Writing a MATLAB program	41
IV.3.1.4 Interests	41
IV.3.1.5 Disadvantages	41
IV.4 OVERVIEW OF THE APPLICATION	41
IV.4.1 <i>Graphic Interface Users</i>	41
IV.4.2 <i>Database</i>	42
IV.4.3 <i>Code of Application</i>	43
IV.4.3.1 Step 1: (Take Picture)	43
IV.4.3.2 Step 2: (Detect Face).....	45
IV.4.3.3 Step 3: (Training)	46
IV.4.3.4 Step 4: (authentication).....	46
IV.5 CONCLUSION	48
GENERAL CONCLUSION	49
BIBLIOGRAPHY	50

LIST OF ABBREVIATIONS

- DNA** : Deoxyribonucleic Acid.
- API** : Application Programming Interface.
- SDK** : Software Development Kit.
- IBG** : International Biometric Groupe.
- FRR** : False Rejection Rate.
- FAR** : False Acceptance Rate.
- EER** : Equal Error Rate.
- ATM** : Automated Teller Machine.
- ID** : Identification.
- PCA** : Principal Components Analysis.
- NN** : Neural Network.
- PNN** : Probabilistic Neural Network.
- SOM** : Self-Organizing Map.
- HMM** : Hidden Markov Model.
- SVM** : Support Vector Machine.
- ICA** : Independent Component Analysis.
- CNN** : Convolution Neural Network.
- AI** : Artificial Intelligence.
- GUI** : Graphic User Interface.

LIST OF FIGURES & TABLES

CHAPTER I: BIOMETRIC TECHNOLOGY

Figure I.1 The different biometric modalities	3
Figure I.2 Iris Picture	4
Figure I.3 Finger print picture	5
Figure I.4 Facial Recognition.....	6
Figure I.5 Vein Recognition.....	6
Figure I.6 Keystroke Dynamics	7
Figure I.7 Vocal (Speech) Recognition.....	7
Figure I.8 Signature Recognition System	8
Figure I.9 DNA Image	9
Figure I.10 Blood Recognition.....	10

CHAPTER II: FACIAL RECOGNITION

Figure II.1 Facial Recognition	16
Figure II.2 Facial Recognition Steps	17
Figure II.3 Face Data Base	22
Figure II.4 Eigen Face	22
Figure II.5 Gabor representation of Human face	23
Figure II.6 Significant facial features and states of 5-state HMM.....	24
Figure II.7 Support Vector Machine (SVM)	25

CHAPTER III: FACE DETECTION THE VIOLA-JONES

METHOD

Figure III.1 Algorithm Flow.....	31
Figure III.2 Detection Faces 1	32
Figure III.3 Detection Faces 2	32

Figure III.4 Haar cascade feature	33
Figure III.5 Haar feature selection.....	33
Figure III.6 Regular Image	34
Figure III.7 Integral Image	35
Figure III.8 Equation of Adaboost.....	36
Figure III.9 Adaboost training	36
Figure III.10 Cascade classifier	37

Chapter IV: Application with GUI MATLAB

Figure IV.1 MATLAB 2020a	40
Figure IV.2 MATLAB GUI of Biometric Recognition	42
Figure IV.3 GUI after created user name.....	43
Figure IV.4 Face Detection.....	44
Figure IV.5 GUI Operation Completed	44
Figure IV.6 Database	46
Figure IV.7 Camera no detected face.....	47
Figure IV.8 Authentication of new user.....	48

CHAPTER I: BIOMETRIC TECHNOLOGY

Table I-1 Applications of Biometrics	14
---	----

GENERAL INTRODUCTION

Now a day, people are using combinations of alphabets and numbers as their secret code to access their account. Although the passwords are unique, the safety cannot be guaranteed as it can easily be forgotten or stolen by identity fraud criminals. Biometric is a method to identify individuals by unique biological traits that individual possesses such as:

- ❖ features of face.
- ❖ finger print and finger vein.
- ❖ Iris.
- ❖ blood type, DNA and many more recognition.

Using these biometric traits provides high security since an account cannot be accessed by any other individuals without the presence of the account owner. Face recognition identify individuals by the features of the face i.e., eyes, nose, mouth, cheekbones, jaws or skin color. Face recognition remains a challenging biometric problem since no technique could provide a robust solution to all situations such as variation of facial expression, pose invariant, illumination invariant, and occlusion among others. Biometric has a wide range application especially in surveillance, security monitoring, immigration, any other applications for identification and recognition [1].

A fingerprint-based biometric system is essentially a pattern recognition system that recognizes a person by determining the authenticity of her fingerprint. Depending on the application context, a fingerprint-based biometric system may be called either a verification system or an identification system:

- ❖ A verification system authenticates a person's identity by comparing the captured fingerprints with her own biometric template(s) pre-stored in the system. It conducts one-to-one comparison to determine whether the identity claimed by the individual is true.
- ❖ An identification system recognizes an individual by searching the entire template database for a match. It conducts one-to-many comparisons to establish the identity of the individual. Throughout this paper the generic term recognition is used where it is not necessary distinguishing between verification and identification [2].

Biometrics accurately identify each individual and distinguishes one from another. Iris recognition is one of important biometric recognition approach in a human identification is becoming very active topic in research and practical application. Iris region is the part between the pupil and the white sclera. This field is sometimes called iris texture. The iris texture provides many minute characteristics such as freckles, coronas, stripes, furrows, crypts, etc. These visible characteristics are unique for each subject. The human iris is not changeable and is stable. From one year of age until death, the patterns of the iris are relatively constant over a person's lifetime [3-6]. Because of this uniqueness and stability, iris recognition is a reliable human identification technique.

Our main goal was to present biometric recognition and types that we talked about in this introduction divided into chapters represented in:

- ❖ Chapter 01: Is the first chapter of our work and it is about Biometric technology
- ❖ Chapter 02: The next one is about facial recognition with details
- ❖ Chapter 03: We will talk about the method used to accomplish the practical work
- ❖ Chapter 04: And finally, we will present to you the practical work represented in algorithm that summarizes our work presented. We used GUI MATLAB

After more than 20 years of development, MATLAB has evolved from a powerful matrix calculation application into a universal programming tool used extensively within scientific and engineering communities both commercial and academic. MATLAB versions 6. x and 7. x include functionality for developing advanced graphical user interfaces, GUI's one of them [7].

CHAPTER I: *Biometric Technology*

I.1 Introduction

Biometric is determined from two Greek words. Bio implies life and Metric implies to measure. There are a few characteristics such as Finger, Iris, Ear, face, Hand Geometry etc., which are most broadly used Biometrics. [1]

A biometric system gives programmed acknowledgment of a person based on a few sorts of interesting highlight or characteristic had by the person.

Biometric system work by to begin with capturing a test of the include, such as recording an advanced sound flag for voice recognition, or taking a computerized color picture for face acknowledgment. The test is at that point changed using a few sorts of scientific work into a biometric format.

Most biometric technology allows two modes of operation, an enrolment mode for including formats to a database, and an identification mode, where a layout is made for a person and after that a match is looked for within the database of pre-enrolled layouts.

I.2 Biometric

I.2.1 Definition

Biometric is an emerging field where technology moves forward our capacity to recognize a person, for customer security against extortion or robbery is one of the objectives of biometrics. First biometric is a mathematical study of the biological variations inside determined group [9],

We have three categories of biometric technology such as morphological analysis which contains (fingerprints, Iris recognition, face recognition, Vein...), A second biometric technology uses biological analysis (smell, blood group, saliva, urine, DNA analysis, etc.), and lately the Behavioral analysis such as keystroke dynamics, vocal recognition, signature dynamics.

The advantage of biometric identification is that each individual has their own physical characteristics which cannot be changed, lost or stolen.

I.2.2 Biometric Characteristics

Biometrics has many characteristics, the most important of it are what we will mention below:

- ❖ **Multi biometric:** The solution supports fingerprint, face, iris and palm print biometric modalities.
- ❖ **Performance:** Designed for fast processing of multiple biometric operations with high accuracy and reliability.
- ❖ **Unlimited storage:** Store biometric and demographic information for unlimited number of people. A single personal record can contain any number of biometric records.
- ❖ **Flexible:** Customable personal record structure (biometric data and demographic data fields), adjustable identity management and adjudication workflows.
- ❖ **Live-capturing:** Supports wide range of biometric devices, including fingerprint and palm print readers, iris scanners, Web and IP cameras.
- ❖ **Easy integration:** Web service-based RESTful API designed for easy and quick integration with third-party systems. Additionally, Java and .NET SDK libraries are provided.
- ❖ **Security:** Role-based access control based on industry-standard authentication mechanisms. System activities are assessable for audit [8].



I.2.3 The different biometric modalities

As we mentioned earlier biometrics is divided into three sections, as shown in the following Figure I.1:

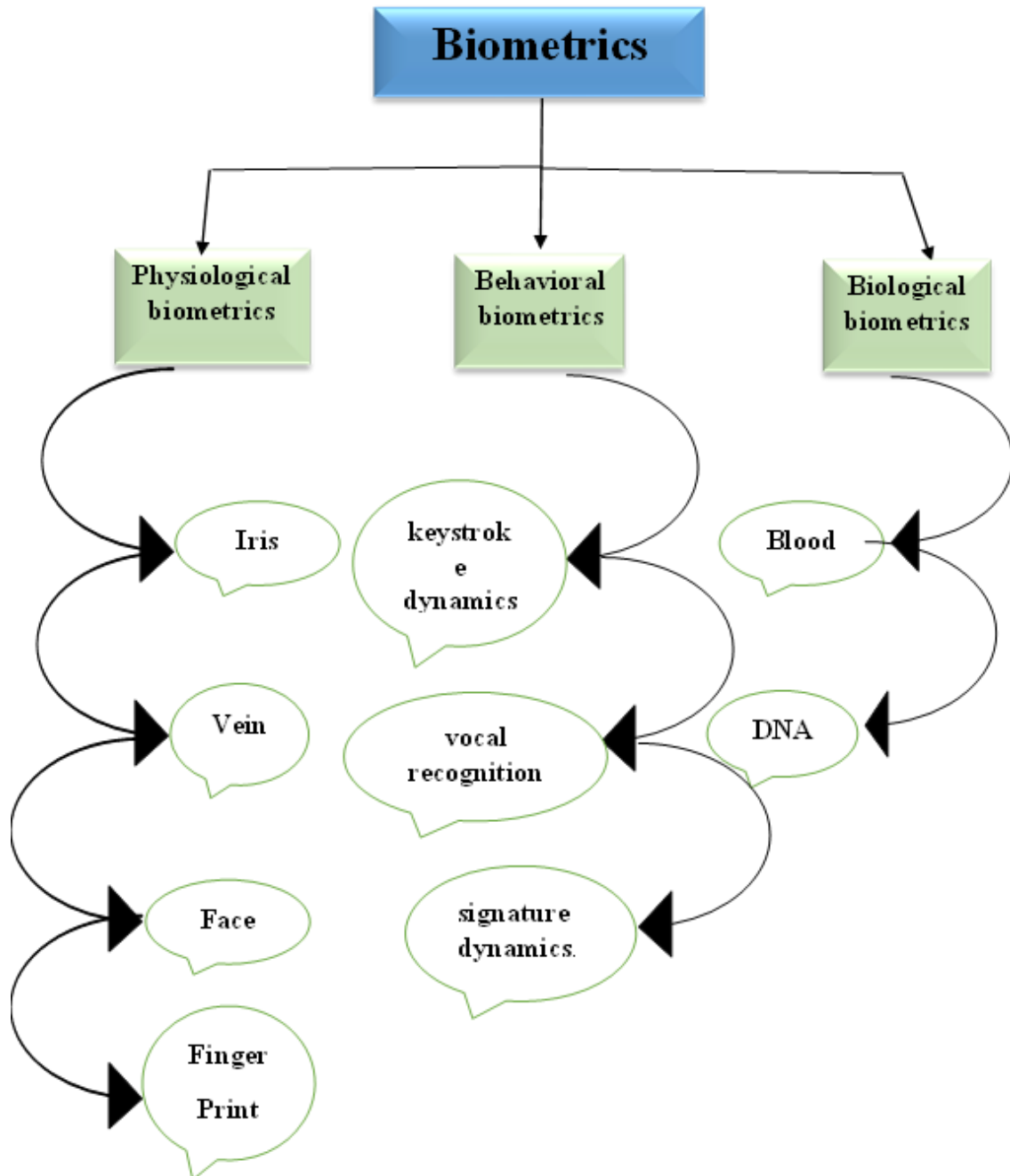


Figure I.1 The different biometric modalities

I.2.3.1 Physiological Biometrics

I.2.3.1.1 Iris:

A. Iris Cameras:

They perform recognition detection of a person's identity by mathematical analysis of the random patterns that are visible within the iris of an eye from some distance. It combines computer vision, pattern recognition, statistical inference, and optics.

B. Iris recognition:

This is rarely impeded by glasses or contact lenses and can be scanned from 10 cm to a few meters away. The iris remains stable over time as long as there are no injuries, and a single enrollment scan can last a lifetime [13].

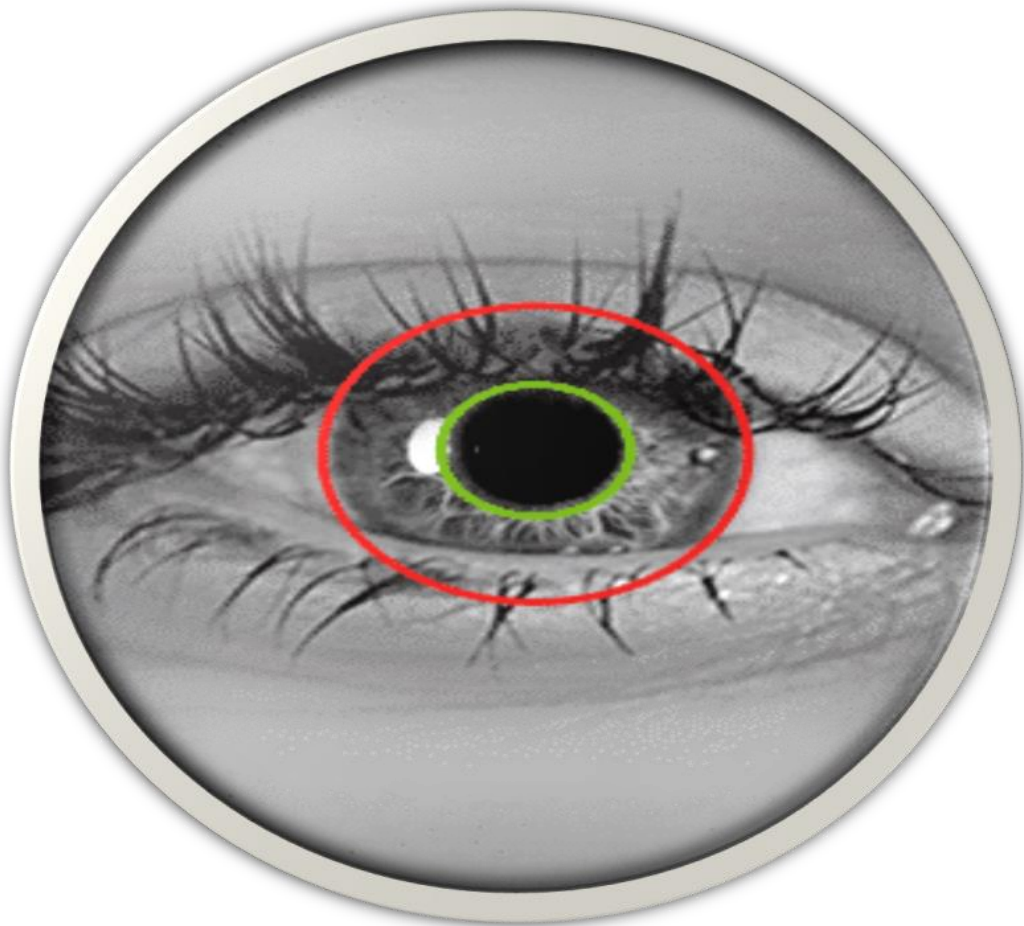


Figure 1.2 Iris Picture

I.2.3.1.2 Finger Prints

Formed when the friction ridges of the skin come in contact with a surface that is receptive to a print by using an agent to form the print, such perspiration, oil, ink, grease, and so forth. The agent is transferred to the surface and leaves an impression which forms the fingerprint [13].



Figure I.3 Finger print picture

I.2.3.1.3 Facial Recognition

This views an image or video of a person and compares it to one in the database. It does this by comparing structure, shape, and proportions of the face, distance between the eyes, nose, mouth, and jaw; upper outlines of the eye sockets, the sides of the mouth, the location of the nose and eyes, and the area surrounding the cheek bones. The main facial recognition methods are feature analysis, neural network and automatic face processing [13].

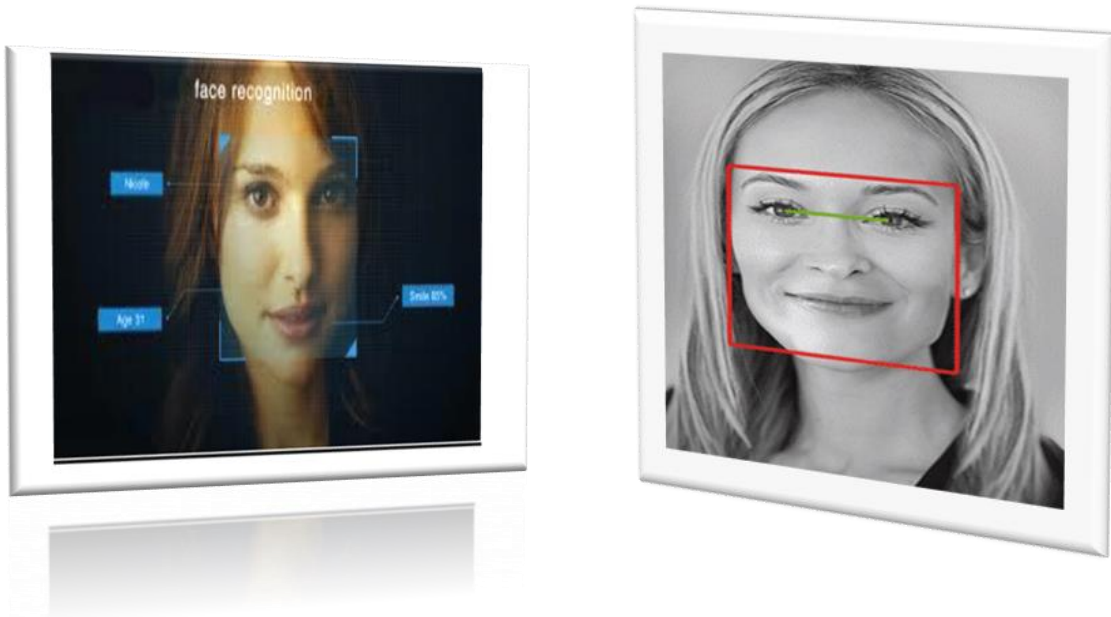


Figure I.4 Facial Recognition

I.2.3.1.4 Vein Recognition

Vein recognition is a type of biometrics that can be used to identify individuals based on the vein patterns in the human finger [13].



Figure I.5 Vein Recognition

I.2.3.2 Behavioral Biometrics

I.2.3.2.1 Keystroke Dynamics

The behavioral biometric Keystroke Dynamics uses the manner and rhythm in which an individual types characters on a keyboard or keypad [10].



Figure I.6 Keystroke Dynamics

I.2.3.2.2 Vocal (Speech) Recognition

Speech recognition is an interdisciplinary subfield of computer science and computational linguistic that develops methodologies and technologies that enable the recognition and translation of spoken language into text by computers [10].



Figure I.7 Vocal (Speech) Recognition

I.2.3.2.3 Signature Dynamics

In this case, more accentuation is given on the behavioral designs in which the signature is marked than the way a signature looks in terms of graphics.

The behavioral designs incorporate the changes within the timing of composing, delays, weight, course of strokes, and speed amid the course of marking.

It can be easy to duplicate the graphical appearance of the signature but it isn't simple to mimic the signature with the same behavior the individual appears whereas signing. This innovation comprises of a write and a specialized composing tablet, both associated to a computer for layout comparison and confirmation.

A tall quality tablet can capture the behavioral characteristics such as speed, weight, and timing whereas marking [13].

Amid enrollment stage, the candidate must sign on the composing tablet different times for information securing. The signature acknowledgment calculations at that point extricates the one-of-a-kind highlights such as timing, weight, speed, heading of strokes, imperative focuses on the way of signature, and the measure of signature.

The calculation relegates diverse values of weights to those points. At the time of distinguishing proof, the candidate enters the live test of the signature, which is compared with the marks within the database [13].



Figure I.8 Signature Recognition System

I.2.3.3 Biological biometrics

I.2.3.3.1 Deoxyribonucleic Acid (DNA)

DNA (Deoxyribonucleic acid) is a chemical substance found in each of the approximately 100 trillion cells within the human body. It contains informational, genetic code for replicating the cells and constructing the proteins required to sustain and develop life.

The entire DNA in each cell holds the complete set of biological instructions for creating an organism and is known as the genome. DNA found in the nucleus of the cell is divided into two chromosomes (one inherited from the mother and the other from the father) and this DNA material comprises both protein-coding regions and non-coding regions. A protein-coding region is known as a gene and this contains all the information for the cell to make proteins. Genes form less than 5% of the genome which is mostly made up from non-coding DNA [14].



Figure I.9 DNA Image

I.2.3.3.2 Blood

In front of a presumed trace of blood, it is necessary first to determine if it is indeed blood, then if it is human blood before trying to identify its owner. The characterization of blood has benefited from the work of many researchers.

Identification of the human origin of a bloodstain is determined by immunological methods. The use of specific serum capable of agglutinating or specifically precipitating elements of human blood makes it possible to distinguish it from the blood of other animals [11].

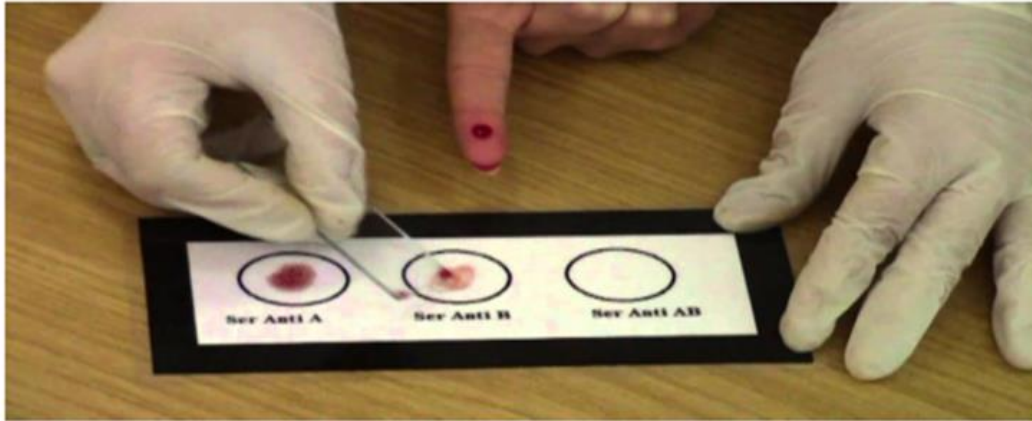


Figure I.10 Blood Recognition

I.3 Biometric Systems

I.3.1 Definition

A biometric system is basically a pattern recognition system that uses an individual's biometric data. Depending on the context of the application, a biometric system can operate in enrollment mode or in authentication mode or in identification mode [12].

❖ **Enrollment mode:**

The enrollment mode is a learning phase which collect biometric information on the people to be identified. Several data acquisition campaigns can be carried out in order to ensure a certain robustness of the recognition system to temporal variations of the data. During this phase, the biometric characteristics of individuals are captured by a biometric sensor, then represented in digital form (signatures), and finally stored in the database. The processing related to enrollment has no time constraint, since it is carried out “offline”.

❖ **Authentication mode:**

Authentication mode is a "one-to-one" comparison, in which the system validates a person's identity by comparing the entered biometric data with that person's biometric template stored in the system's database. In such a mode, the system must then answer the following question: "Am I really the person I am proclaiming?". Currently verification is performed via a personal identification number, a user name, or a smart card.

❖ **Identification mode:**

Identification mode is a "one to N" comparison, in which the system recognizes an individual by matching it with one of the models in the database. The person may not be in the database. This mode consists of associating an identity with a person. In other words, it answers questions like, "Who am I? ".

I.3.2 Biometric System Modules

❖ **Sensor Module:**

This is an appropriate biometric reader or scanner which is essential in the acquisition of the original biometric data of an individual. To take fingerprint images, an ophthalmic fingerprint sensor may be used to copy the friction convexity structure of the fingertip. The sensor module ascertains the human-machine boundary hence critical to the presentation of the biometric system. A scantily designed boundary can result in a high failure to acquire rate and consequently, low user acceptability.

Since most biometric modalities are acquired as images except voice and odor, the quality of the raw data is also impacted by the characteristics of the camera technology that is used [15].

❖ **Quality assessment and feature extraction module:**

The character of the biometric information obtained by the sensor is first gauged to verify its quality for further processing. Normally, the obtained data is submitted to a signal enhancement algorithm to improve its quality. However, in some cases, the quality of the data may be so underprivileged that the user is requested to present the biometric data again. The biometric data is then processed and a deposit of relevant unfair features is reduced to represent the underlying trait [15].

❖ **Matching and decision-making module:**

The extorted features are examined against the stored templates to give match scores. In a fingerprint-based biometric system, the number of identical details between the amount and the template feature sets is determined and a match score is reported. The match score may be controlled by the quality of the presented biometric data. The matcher module also summarizes a decision-making module, in which the match score is used to either authenticate an asserted identity or provide a ranking of the enrolled identities to identify an individual [15].

❖ **System Database Module:**

The database performs as the depository of biometric information. During the staffing process, the feature set extracted from the raw biometric sample is stored in the database together with some biographic information such as Personal Identification Number, characterizing the user.

The data retrieved in the registration method is likely to be controlled by an individual relying on the submission. For example, a user trying to create a new computer account in her biometric-enabled workstation may proceed to enroll her biometrics without any supervision, a person desiring to use a biometric-enabled ATM, on the other hand, will have to enroll her biometrics in the presence of a bank officer after presenting her non-biometric credentials [15].

I.3.3 Performance evaluation of biometric systems

Each biometric feature (or modality) has its strengths and weaknesses, and the choice depends on the intended application. No single biometric modality is expected to effectively meet the requirements of all applications. In other words, no biometric system is "optimal". Matching an application-specific biometric system depends on the operational mode of the application and the biometric characteristics chosen.

Several studies have been conducted to assess the performance of biometric systems. The American company – the International Biometric Group [IBG] – has for example carried out a study based on four evaluation criteria:

- ❖ **Intrusiveness:** this criterion makes it possible to classify biometric systems according to the existence of direct contact between the sensor used and the individual to be recognized. Face recognition is a "non-intrusive" technique, because there is no contact between the sensor (the camera) and the subject, it is well accepted by users unlike other "intrusive" techniques such as iris where direct contact is required between the sensor and the eye.
- ❖ **Reliability:** depends on the quality of the environment (lighting for example) in which the user finds himself. This criterion influences the recognition of the user by the system.
- ❖ **Cost:** should be moderate. In this regard we can say that facial recognition does not require expensive technology. Indeed, most systems operate using a standard quality digital camera.

- ❖ **Effort:** required by the user when entering biometric measurements, and which should be reduced as much as possible. Facial recognition is the easiest biometric technique to use because it is non-binding [12].

I.3.4 Reliability of biometric systems

In order to measure the reliability of a biometric system in verification and/or identification mode, two main tests are used [12].

1. Verification Test:

In the verification task, an end user must request authentication of their identity. For example: he proclaims "I am Mr. Smith", then the biometric system must determine whether the identity proclaimed by the user is accepted or rejected. Two rates are then calculated

- ❖ **The False-Rejection Rate (FRR)**, it expresses the percentage of users rejected when they should be accepted by the system.

$$FRR = \frac{\text{number of rejected users}}{\text{total number of users accesses}} \quad (\text{CHAPTER I:.1})$$

- ❖ **The False Acceptance Rate (FAR)**, it expresses the percentage of users accepted by the system when they should be rejected.

$$FAR = \frac{\text{number of impostors accepted}}{\text{total number of impostor accesses}} \quad (\text{CHAPTER I:.2})$$

- ❖ **The Equal Error Rate (EER)**, it is calculated from the first two criteria and is a common performance measurement point. This point corresponds to where $FRR = FAR$, i.e., the best compromise between false rejects and false accepts.

2. Identification Test

The identification test is the most commonly used measure, but it is not always sufficient. Indeed, in case of error, it can be useful to know if the right choice is among the first N answers of the system.

I.3.5 Application of Biometrics

Ascertaining the uniqueness of a person with high confidence is becoming essential in several functions in our widely consistent society. Methods of consistent authentication have

dramatically enhanced security, and fast developments in global connection, the activity of conveying information. Thus, biometrics is being progressively more integrated into several different applications. These applications can be categorized into the following groups [16].

1. Commercial applications such as computer network login, electronic data security, e-commerce, internet access, ATM, or credit card use.
2. Government applications such as national ID card, managing inmates in a correctional facility, driver's license, social security, welfare-disbursement, border control, and passport control.
3. Forensic applications such as corpse identification, criminal investigation, and parenthood determination and parenthood determination.

Table I-1 Applications of Biometrics

FORENSICS	GOVERNMENT	COMMERCIAL
Corpse Identification	National ID	ATM
Criminal Investigation	Driver's license	Access control
Parenthood determination	Welfare disbursement	Mobile phone
Missing children	Border crossing	E-Commerce, Internet, Banking, Smart Card

I.4 Conclusion

In this first chapter, we talked in detail about biometrics. We first started with the definition that led us to the characteristics and types of biometrics, then we touched on the biometric system and the various technologies used in it to identify people, facilitate the process and protect information.

We knew very well that biometrics has become a very important technology in human life, and dispensing with it or ignoring it is rejected. Rather, it must be developed more and more.

In the coming chapters, it will become clear to us more about its importance and where its application can lead to human progress.

CHAPTER II: *Facial Recognition*

II.1 Introduction

With the rapid development in the field of pattern recognition and its uses in different areas e.g., facial recognition, signature recognition, arises the importance of the utilization of this technology in different areas in large organizations.

This is mainly because these applications help the top-management take decisions that improve the performance and effectiveness of the organization. On the other hand, for an organization to be effective, it needs accurate and fast means of recording the performance of the people inside this organization.

Biometric recognition has the potential to become an irreplaceable part of many identification systems used for evaluating the performance of those people working within the organization. Although biometric technologies are being applied in many fields it has not yet delivered its promise of guaranteeing automatic human recognition. [18]

Biometric technologies may seem exotic, but their use is becoming increasingly common, and in 2001 MIT Technology Review named biometrics as one of the “top ten emerging technologies that will change the world.” While this chapter focuses on facial recognition although there were many different types of biometrics. [19]

II.2 Facial Recognition

II.2.1 Definition

Face recognition is a technique of biometric recognition. It is considered to be one of the most successful applications of image analysis and processing; that is the main reason behind the great attention it has been given in the past several years. [18]

Facial recognition offers several advantages. The system captures face of people in public areas, which minimizes legal concerns for reasons explained below. Moreover, since faces can be captured from some distance away, facial recognition can be done without any physical contact. This feature also gives facial recognition a clandestine or covert capability. [19]

The facial recognition process is similar to the general biometric recognition process, in the face-base biometric systems detection; alignment, feature extraction, and matching take place. The facial recognition process can be divided into two main stages: processing before detection where face detection and alignment take place (localization and normalization), and afterwards recognition occur through feature extraction and matching steps. [18-19]



Figure II.1 Facial Recognition

II.2.2 Facial Recognition Steps

A. Face Detection (Capture Image):

First, an image of the face is acquired. This acquisition can be accomplished by digitally scanning an existing photograph or by using an electro-optical camera to acquire a live picture of a subject. As video is a rapid sequence of individual still images, it can also be used as a source of facial images. [19]

B. Face Alignment (Find Face in Image):

This process focuses on finding the best localization and normalization of the face; where the detection step roughly estimates the position of the face, this step outlines the facial components, such as face outline, eyes, nose, ears and mouth. Afterwards normalization with respect to geometrical transforms such as size and pose, in addition to photometrical properties such as illumination and grey scale take place. [18]

C. Extract feature (to generate template)

After the previous two steps, feature extraction is performed resulting in effective information that is useful for distinguishing between faces of different persons and stable with respect to the geometrical and photometrical variations. [18]

D. Compare Templates (Feature Matching)

The fourth step is to compare the template generated in step three with those in a database of known faces. In an identification application, this process yields scores that indicate how closely the generated template matches each of those in the database. In a verification application, the generated template is only compared with one template in the database – that of the claimed identity. [19]

E. Declare Matches (Database of Enrolled Users)

The final step is determining whether any scores produced in step four are high enough to declare a match. The rules governing the declaration of a match are often configurable by the end user, so that he or she can determine how the facial recognition system should behave based on security and operational considerations. [19]

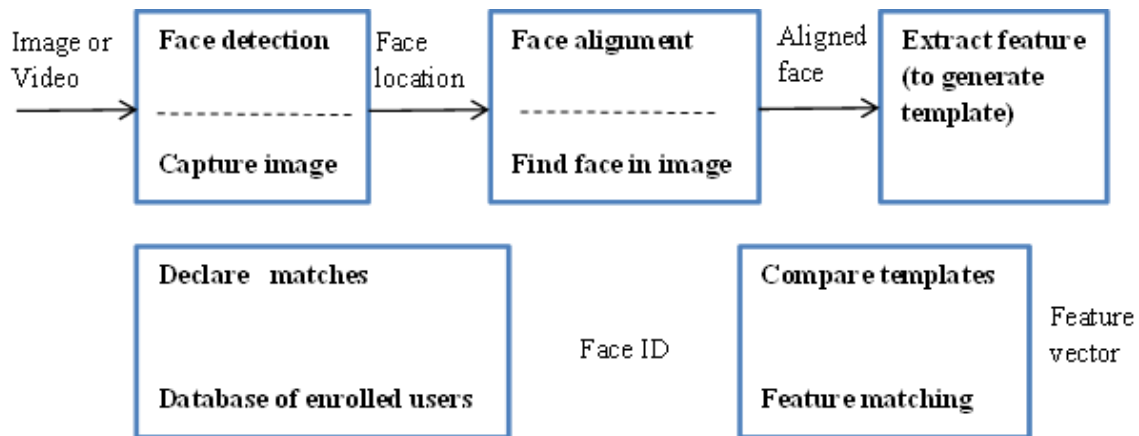


Figure II.2 Facial Recognition Steps

II.2.3 Application of facial recognition

Automatic face recognition techniques have been utilized in many applications over the past years. [20]

❖ Security:

Facial recognition is used to identify when known shoplifters, organized retail criminals, or people with a history of fraud enter stores. Photographs of individuals

can be matched against large databases of criminals so that loss prevention and retail security professionals can be notified when shoppers who potentially represent a threat enter the store.

❖ **Unlocking Phones:**

Various phones, including the most recent iPhones, use face recognition to unlock the device. The technology offers a powerful way to protect personal data and ensures that sensitive data remains inaccessible if the phone is stolen. Apple claims that the chance of a random face unlocking your phone is about one in 1 million.

❖ **Law Enforcement:**

Facial recognition is regularly being used by law enforcement. According to this NBC report the technology is increasing amongst law enforcement agencies within the US, and the same is true in other countries. Police collects mugshots from arrestees and compare them against local, state, and federal face recognition databases. Once an arrestee's photo has been taken, their picture will be added to databases to be scanned whenever police carry out another criminal search.

Also, mobile face recognition allows officers to use smartphones, tablets, or other portable devices to take a photo of a driver or a pedestrian in the field and immediately compare that photo against to one or more face recognition databases to attempt an identification.

❖ **Airports and Border Control:**

Facial recognition has become a familiar sight at many airports around the world. Increasing numbers of travellers hold biometric passports, which allow them to skip the ordinarily long lines and instead walk through an automated ePassport control to reach the gate faster. Facial recognition not only reduces waiting times but also allows airports to improve security. The US Department of Homeland Security predicts that facial recognition will be used on 97 per cent of travellers by 2023. As well as at airports and border crossings, the technology is used to enhance security at large-scale events such as the Olympics.

❖ **Finding Missing Persons:**

Facial recognition can be used to find missing persons and victims of human trafficking. Suppose missing individuals are added to a database. In that case, law enforcement can be alerted as soon as they are recognized by face recognition whether it is in an airport, retail store, or other public space.

❖ **Banking:**

Biometric online banking is another benefit of face recognition. Instead of using one-time passwords, customers can authorize transactions by looking at their smartphone or computer. With facial recognition, there are no passwords for hackers to compromise. If hackers steal your photo database, 'liveless' detection – a technique used to determine whether the source of a biometric sample is a live human being or a fake representation – should (in theory) prevent them from using it for impersonation purposes. Face recognition could make debit cards and signatures a thing of the past.

❖ **Marketing and Advertising:**

Marketers have used facial recognition to enhance consumer experiences. For example, frozen pizza brand DiGiorno used facial recognition for a 2017 marketing campaign where it analyzed the expressions of people at DiGiorno-themed parties to gauge people's emotional reactions to pizza. Media companies also use facial recognition to test audience reaction to movie trailers, characters in TV pilots, and optimal placement of TV promotions. Billboards that incorporate face recognition technology – such as London's Piccadilly Circus – means brands can trigger tailored advertisements.

❖ **Healthcare:**

Hospitals use facial recognition to help with patient care. Healthcare providers are testing the use of facial recognition to access patient records, streamline patient registration, detect emotion and pain in patients, and even help to identify specific genetic diseases. AiCure has developed an app that uses facial recognition to ensure that people take their medication as prescribed. As biometric technology becomes less expensive, adoption within the healthcare sector is expected to increase.

❖ **Recognizing drivers:**

According to this consumer report, car companies are experimenting with facial recognition to replace car keys. The technology would replace the key to access and start the car and remember drivers' preferences for seat and mirror positions and radio station presets. [20]

II.2.4 Examples of facial recognition technology

1. **Amazon:**

Previously promoted its cloud-based face recognition service named 'Rekognition' to law enforcement agencies. However, the company announced it was planning a one-

year moratorium on the use of its technology by police. The rationale for this was to allow time for US federal laws to be initiated, to protect human rights and civil liberties.

2. Apple:

Uses facial recognition to help users quickly unlock their phones, log in to apps, and make purchases.

3. British Airways:

Enables facial recognition for passengers boarding flights from the US. Travellers' faces can be scanned by a camera to have their identity verified to board their plane without showing their passport or boarding pass. The airline has been using the technology on UK domestic flights from Heathrow and is working towards biometric boarding on international flights from the airport.

4. Coca-Cola:

Has used facial recognition in several ways across the world. Examples include rewarding customers for recycling at some of its vending machines in China, delivering personalized ads on its vending machines in Australia.

5. Facebook:

Began using facial recognition in the US in 2010 when it automatically tagged people in photos using its tag suggestions tool. The tool scans a user's face and offers suggestions about who that person is. Since 2019, Facebook has made the feature opt in as part of a drive to become more privacy focused. Facebook provides information on how you can opt-in or out of face recognition [here](#).

6. Google:

Incorporates the technology into Google Photos and uses it to sort pictures and automatically tag them based on the people recognized.

7. MAC make-up:

Uses facial recognition technology in some of its brick-and-mortar stores, allowing customers to virtually "try on" make-up using in store augmented reality mirrors.

8. McDonald's:

Has used facial recognition in its Japanese restaurants to assess the quality of customer service provided there, including analyzing whether its employees are smiling while assisting customers.

9. Snapchat:

Is one of the pioneers of facial recognition software: it allows brands and organizations to create filters which would to the user's face hence the ubiquitous puppy dog faces and flower crown filters seen on social media. [20]

II.3 Face Recognition Methods

II.3.1 Eigen Face

Eigen face technique is among one of the face recognition methodologies. This method is also called as Eigen Vector or Principal Component Analysis (PCA). Distinctions among multiple faces are measured using Eigen Vectors [21]. These Eigen Vectors [22] are computed from Covariance Matrix. Computing the Eigen Vector and Eigen Values from Covariance Matrix of the high dimensional vector space is known as PCA. These constructed Eigen faces describe each face. These Eigen faces are computed by measuring the distance between key features of the human faces. These key features include nose tip, mouth and eye corners and chin edges.

The Eigen face method was introduced by Sirovich and Kirby in 1987 [23]. Later this methodology was successfully used by Turk and Pentland [24] for face recognition which is motivated by information theory. PCA reduces the dimensionality of the face space and only the part important for face recognition is left behind. The faces to be tested are projected onto this reduced face space ("feature space"). The figure 2.3 and 2.4 shows the face database, and Eigen faces.



Figure II.3 Face Data Base



Figure II.4 Eigen Face

II.3.2 Gabor Wavelet

Gabor wavelet is also known as Gabor Filter. Gabor filters were introduced as a tool for signal processing in noise by Dennis Gabor in 1946. Gabor Filters were presented for 1-D Signals by Dennis Gabor, Later Daugman rediscovered and generalized them to 2-D Gabor Filters [25]. Gabor wavelet method is such a method that uses local features for face recognition. Multi-Oriental information of a face image can be extracted by using the Gabor Wavelets. The features extracted by Gabor are called Gabor Features and these features are in local regions at multiple scales Redundancy is present in Gabor features because these features are usually high dimensional data and sometimes overlapping occurs between the

supports of Gabor filters that result in redundancy of information of features. Feature reduction can be done using Gabor Wavelet transformation method. Face recognition can also be done by using Gabor features in the global form. Gaussian envelope function restricts the Gabor filters.

An image can also be represented by the Gabor wavelet transform allowing the description of both the spatial relations and spatial frequency structure. Gabor Wavelet has a property to allow it to capture the properties of spatial localization, spatial frequency selectivity, and orientation. It extracts edge and shape information. Since the feature-based methods represent the faces in a compact way in a similar way Gabor Wavelet method also represents the faces in a compact way. Figure II.5 shows the 2D Gabor Representations of Human Face.



Fig. 1. Images from the FR/Action of Gabor wavelet transform

Figure II.5 Gabor representation of Human face

II.3.3 Neural Network (NN)

Because of the importance of the face recognition in several fields, different methods are used to accomplish this task. NN consist on some simple elements that operate in parallel. NN can also be used for Facial Emotion Classification and Gender Classification. NN are used because they reduce the complexity. The neural network learns from experience, it works well on the images with varying lighting conditions and improves accuracy. The major disadvantage of the neural network is a large amount of time required for its training. ANN recognizes the face through learning and previous experience. NN based system is trained to recognize the faces. Neural Network in combination with Incremental Learning Ability was also used for the face recognition purpose The Probabilistic Neural Network (PNN) approach was designed by

Vinitha and Santosh that detected and recognized the faces from the grayscale images containing the frontal view of the faces. The main advantage of using PNN is that it requires short training time. The Network in the PNN is divided into subnets because its network is not completely connected. Self-Organizing Map Neural Network (SOM) having the property of topological preservation is an artificial neural network used in face recognition. SOM is also known as Kohonen Map. [26-29]

II.3.4 Hidden Markov Model (HMM)

HMM is a statistical model. The observable properties of a signal are characterized by HMM. This Model has two processes. One of them is Markov Chain with a finite number of states that can't be viewed overtly. While in the other process each state has a set of probability density function associated with it. This model is analogous to Eigen face method. Ever since its introduction in the 1960s, this model contributed a great deal to speech recognition. However, in 1994, it was also used to identify the faces by Samaria and Young for the first time. Now HMM is being used for face recognition, face detection, object recognition but earlier HMM were usually used to deal with one-dimensional data only. Normally 5-state HMM is used in the researches made for face recognition system. 5-state HMM groups the face into 5 facial features i.e. mouth, eyes, nose, chin, forehead for frontal face images [The number of states can be increased or decreased depending upon the system's requirement. Using 7-State HMM adds significant details which enhance the performance of the face recognition system. The Figure II.6 shows the significant facial features and states of 5-state HMM



Figure II.6 Significant facial features and states of 5-state HMM

II.3.5 Support Vector Machine (SVM)

Different methods are used to accomplish the task of classification. SVM is a method that deals well with the issue of classification. As SVM is a machine learning approach in which the classifier is trained that can to effectively deal with the face recognition problem. From the training data, SVM takes out the related discriminatory information. [SVM works to find the classification hyperplane. To apply SVM, the missing entries should not be there in the samples defined by feature vectors. SVM are proposed to deal with the two-class predicament. And Face Recognition is Multi-class problem. SVM can be applied to recognize the faces after facial feature extraction or onto the original appearance space. For face recognition, SVM can be applied individually or can be used with the other techniques. Like a Hybrid method can be used in which features can be extracted via Independent Component Analysis (ICA) and then afterward the recognition issue can be resolved using SVM. This approach to face recognition gives a good result but both methods ICA and SVM are slow in feature selection and classification respectively. Multi-class face recognition matter can be cracked by integrating binary tree recognition approach with SVM. To tackle face recognition Fast Least Squares SVM quickly locates the optimization classification hyperplanes by selecting the training sample points with bigger values directly. [30]

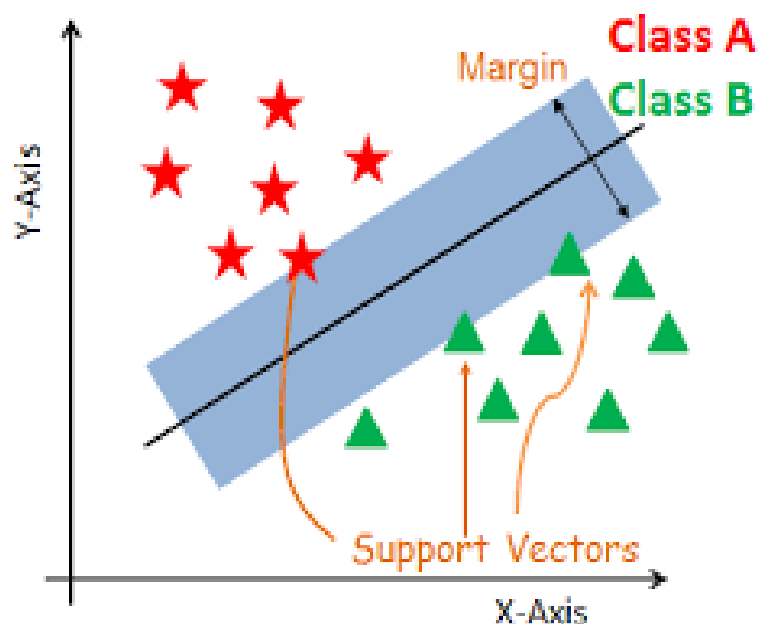


Figure II.7 Support Vector Machine (SVM)

II.4 Advantages and Disadvantages of face recognition

II.4.1 Advantages

❖ **Increased security:**

On a governmental level, facial recognition can help to identify terrorists or other criminals. On a personal level, facial recognition can be used as a security tool for locking personal devices and for personal surveillance cameras.

❖ **Reduced crime:**

Face recognition makes it easier to track down burglars, thieves, and trespassers. The sole knowledge of the presence of a face recognition system can serve as a deterrence, especially to petty crime. Aside from physical security, there are benefits to cybersecurity as well. Companies can use face recognition technology as a substitute for passwords to access computers. In theory, the technology cannot be hacked as there is nothing to steal or change, as is the case with a password.

❖ **Removing Bias from Stop and Search**

Public concern over unjustified stops and searches is a source of controversy for the police — facial recognition technology could improve the process. By singling out suspects among crowds through an automated rather than human process, face recognition technology could help reduce potential bias and decrease stops and searches on law-abiding citizens.

❖ **Greater Convenience**

As the technology becomes more widespread, customers will be able to pay in stores using their face, rather than pulling out their credit cards or cash. This could save time in checkout lines. Since there is no contact required for facial recognition as there is with fingerprinting or other security measures – useful in the post-COVID world – facial recognition offers a quick, automatic, and seamless verification experience.

❖ **Faster Processing**

The process of recognizing a face takes only a second, which has benefits for the companies that use facial recognition. In an era of cyber-attacks and advanced hacking

tools, companies need both secure and fast technologies. Facial recognition enables quick and efficient verification of a person's identity.

❖ **Integration With Other Technologies**

Most facial recognition solutions are compatible with most security software. In fact, it is easily integrated. This limits the amount of additional investment required to implement it. [21]

II.4.2 Disadvantages

While some people do not mind being filmed in public and do not object to the use of facial recognition where there is a clear benefit or rationale, the technology can inspire intense reactions from others. Some of the disadvantages or concerns include:

❖ **Surveillance**

Some worry that the use of facial recognition along with ubiquitous video cameras, artificial intelligence, and data analytics creates the potential for mass surveillance, which could restrict individual freedom. While facial recognition technology allows governments to track down criminals, it could also allow them to track down ordinary and innocent people at any time.

❖ **Scope for error**

Facial recognition data is not free from error, which could lead to people being implicated for crimes they have not committed. For example, a slight change in camera angle or a change in appearance, such as a new hairstyle, could lead to error. In 2018, Newsweek reported that Amazon's facial recognition technology had falsely identified 28 members of the US Congress as people arrested for crimes.

❖ **Breach of privacy**

The question of ethics and privacy is the most contentious one. Governments have been known to store several citizens' pictures without their consent. In 2020, the European Commission said it was considering a ban on facial recognition technology in public spaces for up to five years, to allow time to work out a regulatory framework to prevent privacy and ethical abuses.

❖ **Massive data storage**

Facial recognition software relies on machine learning technology, which requires massive data sets to “learn” to deliver accurate results. Such large data sets require robust data storage. Small and medium-sized companies may not have sufficient resources to store the required data. [22]

II.5 Facial Recognition Security - How to Protect Yourself

While biometric data is generally considered one of the most reliable authentication methods, it also carries significant risk. That’s because if someone’s credit card details are hacked, that person has the option to freeze their credit and take steps to change the personal information that was breached. What do you do if you lose your digital ‘face’?

Around the world, biometric information is being captured, stored, and analyzed in increasing quantities, often by organizations and governments, with a mixed record on cybersecurity. A question increasingly being asked is, how safe is the infrastructure that holds and processes all this data.

As facial recognition software is still in its relative infancy, the laws governing this area are evolving (and sometimes non-existent). Regular citizens whose information is compromised have relatively few legal avenues to pursue. Cybercriminals often elude the authorities or are sentenced years after the fact, while their victims receive no compensation and are left to fend for themselves.

As the use of facial recognition becomes more widespread, the scope for hackers to steal your facial data to commit fraud increases.

A comprehensive cybersecurity package is an essential part of protecting your online privacy and security. We recommend Kaspersky Security Cloud which provides protection for all your devices and includes antivirus, anti-ransomware, mobile security, password management, VPN, and parental controls.

Biometric technology offers very compelling security solutions. Despite the risks, the systems are convenient and hard to duplicate. These systems will continue to develop in the future — the challenge will be to maximize their benefits while minimizing their risks. [20]

II.6 Conclusion

In this chapter the effort is being made to present a review of the face recognition, as it is active research area due to its several benefits. Recent progress in the field of face recognition is covered by conducting a review of a noteworthy number of researchers. Continuous efforts are being made by the researchers in this area, through which encouraging progress is achieved. But still there is the need to make face recognition system that can achieve accurate results under unconstrained environment. Some researchers have used single method while some used hybrid approaches with the common aim to make a system for face recognition with 100% recognition rate.

CHAPTER III: *Face Detection the Viola-Jones Method*

III.1 Introduction

The world of image-processing always shows interesting and amazing techniques for object detection. And face detection using VIOLA-JONES algorithm is one of these fascinating techniques.

Face detection is the first basic step to all the facial analysis methods like face recognition, face alignment, face modeling, face verification and facial tracking etc. To accurately detect faces the computer system requires some training so that the computer system can easily identify whether it's face or non-face. To detect faces, several threshold values have been determined. Based on this value a system can detect human faces [31].

Face detection according to [32] can be categorized into 4 grouping based on the algorithm namely knowledge-based methods, feature invariant methods, template-based methods and appearance-based methods. The appearance-based method uses very large number of examples. This example can be face images or facial features and describe different variations such as face shape, skin color, eye color, closed or open mouth and others. Face detection can be seen as a classification of patterns where the input is the image and the output of the class will be determined from the image. In this case there are two classes, namely face and non-face. During this time many face recognition techniques assume that face data are the same size and uniform background. In reality, this assumption does not always apply because faces can appear in various sizes and image positions with varying backgrounds. Currently there are many applications that use face detection features [33] [34].

Face detection has several applications in our real-life word. The security cameras use these to detect faces and recognize faces of strangers, it can be used also to add filters to the face and enhance portrait modes, recently it has been used to auto-unlock the phone. All of this happens in real time.

Face detection can be done using the Viola-Jones method. Viola Jones algorithm is named after two computer vision researchers who proposed the method in 2001, Paul Viola and Michael Jones in their paper, “Rapid Object Detection using a Boosted Cascade of Simple Features”. Despite being an outdated framework, Viola-Jones is quite powerful, and its application has proven to be exceptionally notable in real-time face detection. This algorithm is painfully slow to train but can detect faces in real-time with impressive speed.

Given an image (this algorithm works on grayscale image), the algorithm looks at many smaller sub regions and tries to find a face by looking for specific features in each sub region. It needs to check many different positions and scales because an image can contain many faces of various sizes. Viola and Jones used Haar features to detect faces in this algorithm. [35]

III.2 Algorithm

The overall flow of the algorithm is as follows (Figure III.1):

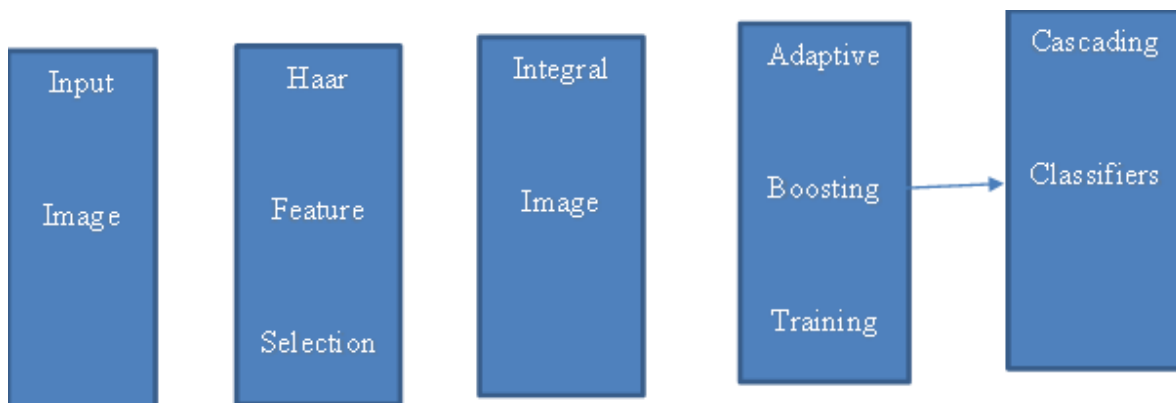


Figure III.1 Algorithm Flow

III.2.1 Input Image

Viola-Jones was designed for frontal faces, so it is able to detect frontal the best rather than faces looking sideways, upwards or downwards. Before detecting a face, the image is converted into grayscale, since it is easier to work with and there's lesser data to process. The Viola-Jones algorithm first detects the face on the grayscale image and then finds the location on the colored image. [36]

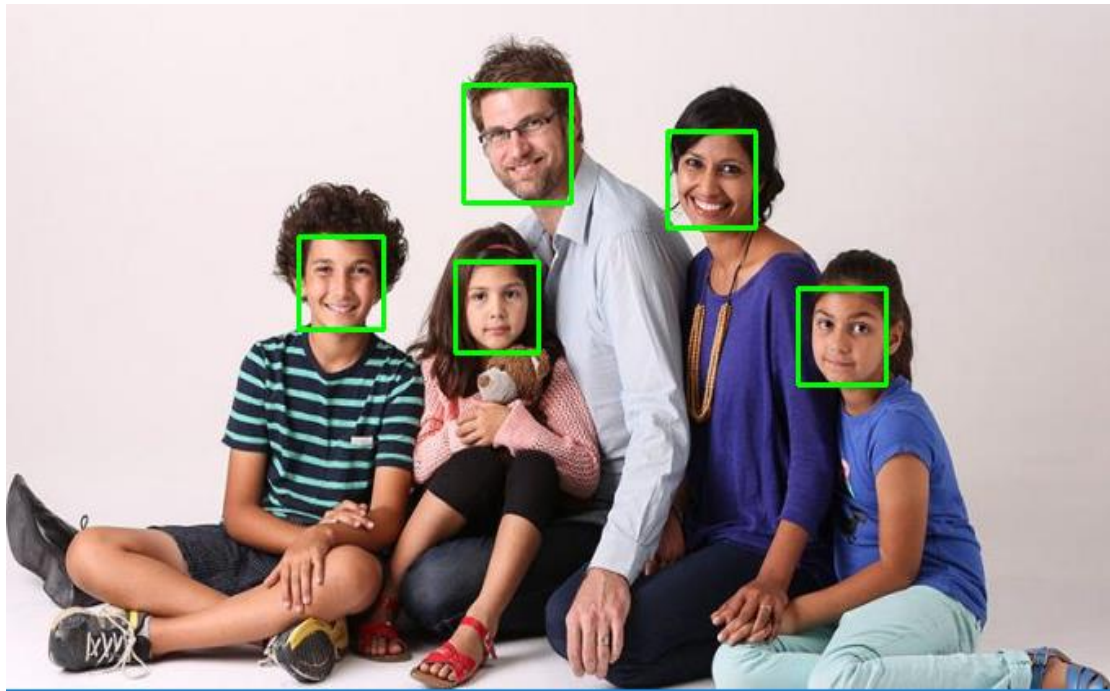


Figure III.2 Detection Faces 1

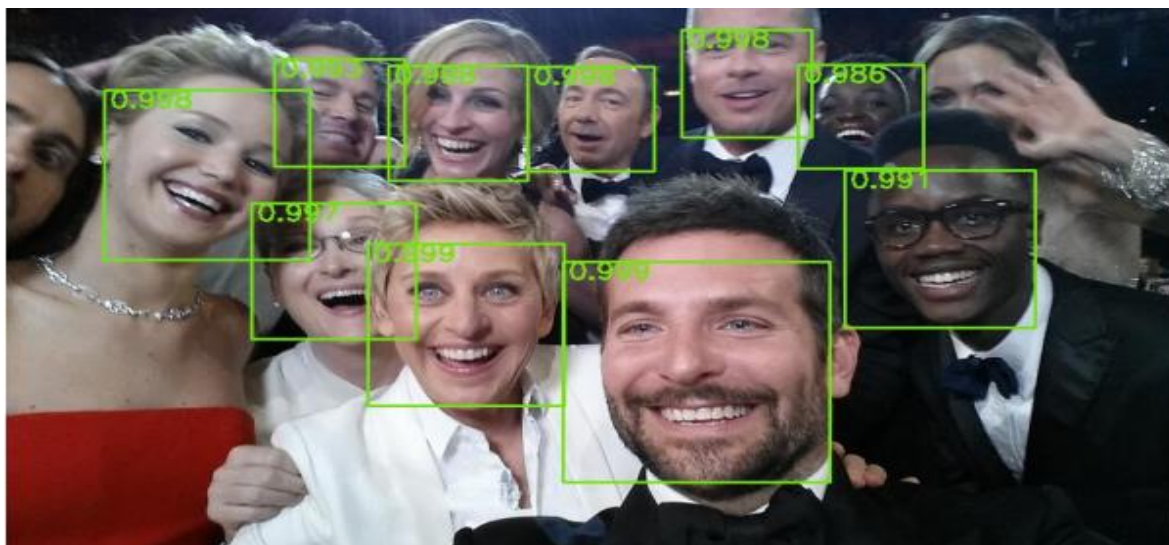


Figure III.3 Detection Faces 2

III.2.2 Haar Feature Selection

Haar features are named after ‘Alfred Haar’, a Hungarian mathematician in the 19th century who developed the concept of Haar wavelets (kind of like the ancestor of haar-like features). The features below show a box with a light side and a dark side, which is how the machine determines what the feature is. Sometimes one side will be lighter than the other, as in an edge of an eyebrow. Sometimes the middle portion may be shinier than the surrounding boxes, which can be interpreted as a nose. [36]

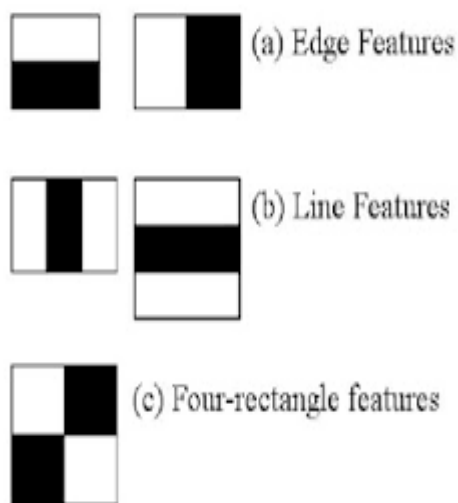


Figure III.4 Haar cascade feature

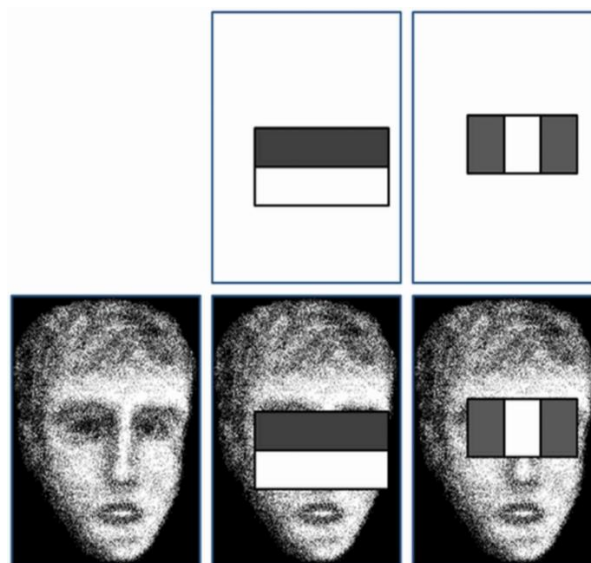


Figure III.5 Haar feature selection

There are 3 types of Haar features selection that Viola and Jones identified in their research:

- ❖ **Edge features**
- ❖ **Line-features**
- ❖ **Four-sided features**

Edge features and Line features are useful for detecting edges and lines respectively. The four-sided features are used for finding diagonal features.

The value of the feature is calculated as a single number: the sum of pixel values in the black area minus the sum of pixel values in the white area. The value is zero for a plain surface in which all the pixels have the same value, and thus, provide no useful information. [36]

Since our faces are of complex shapes with darker and brighter spots, a Haar feature gives you a large number when the areas in the black and white rectangles are very different. Using this value, we get a piece of valid information out of the image.

To be useful, a Haar feature needs to give you a large number, meaning that the areas in the black and white rectangles are very different. There are known features that perform very well to detect human faces:

For example, when we apply this specific haar feature to the bridge of the nose, we get a good response. Similarly, we combine many of these features to understand if an image region contains a human face. [37]

III.2.3 Integral image:

In the previous section, we have seen that to calculate a value for each feature, we need to perform computations on all the pixels inside that particular feature. So in this section, we calculated the value of a feature. In reality, these calculations can be very intensive since the number of pixels would be much greater within a large feature.

The integral image plays its part in allowing us to perform these intensive calculations quickly so we can understand whether a feature of a number of features fit the criteria

8	5	6	4	4	2	3	4	4	3
7	5	6	5	5	6	6	5	5	4
5	5	7	8	9	7	7	6	5	3
2	4	3	3	4	5	6	6	5	4
2	3	4	5	5	6	6	7	5	5

Figure III.6 Regular Image

To calculate the value of a single box in the integral image, we take the sum of all the boxes to its left. The image below shows an example:

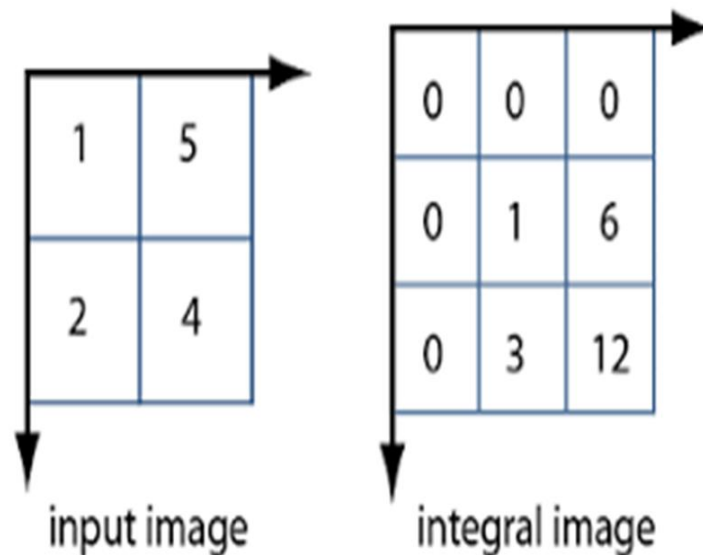



Figure III.7 Integral Image

we use the integral image Because Haar features are actually rectangular, and the integral image process allows us to find a feature within an image very easily as we already know the sum value of a particular square and to find the difference between two rectangles in the regular image, we just need to subtract two squares in the integral image. So even if you had 1000 x 1000 pixels in your grid, the integral image method makes the calculations much less intensive and can save a lot of time for any facial detection model. [36] [37]

III.2.4 Adaptive boosting (Adaboost)

The algorithm learns from the images we supply it and is able to determine the false positives and true negatives in the data, allowing it to be more accurate. We would get a highly accurate model once we have looked at all possible positions and combinations of those features. Training can be super extensive because of all the different possibilities and combinations you would have to check for every single frame or image.

Let's say we have an equation for our features that determines the success rate (as seen in the image (figure 6), with f_1 , f_2 and f_3 as the features and a_1 , a_2 , a_3 as the respective weights of the features. Each of the features is known as a weak classifier. The left side of the equation $F(x)$ is called a strong classifier. Since one weak classifier may not be as good, we get a strong classifier when we have a combination of two or three weak classifiers (figure 8). As you keep adding, it gets stronger and stronger. This is called an ensemble. You want to make sure that you have the most important features in front, but the question is how do you find the most important or the 'best' features? That's where Adaptive Boosting comes into play. [36]



$$F(x) = \alpha_1 f_1(x) + \alpha_2 f_2(x) + \alpha_3 f_3(x) + \dots$$

Figure III.8 Equation of Adaboost

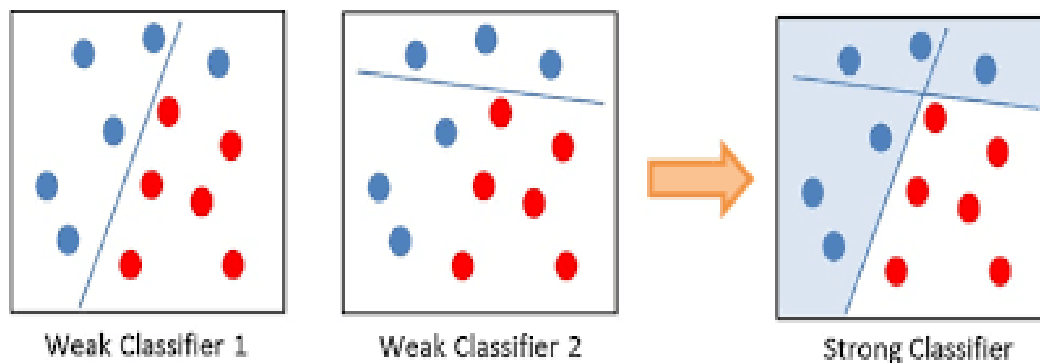


Figure III.9 Adaboost training

when we're training the AdaBoost to identify important features, we're feeding it information in the form of training data and subsequently training it to learn from the information to predict. So ultimately, the algorithm is setting a minimum threshold to determine whether

Adaptive boosting uses another feature, the one to best complement our current strongest feature. So it doesn't look for the second-best feature, but one that complements the current best feature. So it increases the importance of the images that it got wrong as false negatives, and finds the next best feature that would fit these images, in a way, increasing the weight of these images on the overall algorithm. So, as new features are added, we would come down to one image at the end that would be given a higher weight. Once the algorithm is optimized and is able to calculate all positives and negatives correctly, we move on to the next step: cascading. [36][37]

III.2.5 Cascading classifiers

Maybe the AdaBoost will finally select the best features around say 2500, but it is still a time-consuming process to calculate these features for each region. We have a 24×24 window which we slide over the input image, and we need to find if any of those regions contain the face. The job of the cascade is to quickly discard non-faces, and avoid wasting precious time and computations. Thus, achieving the speed necessary for real-time face detection. [36]

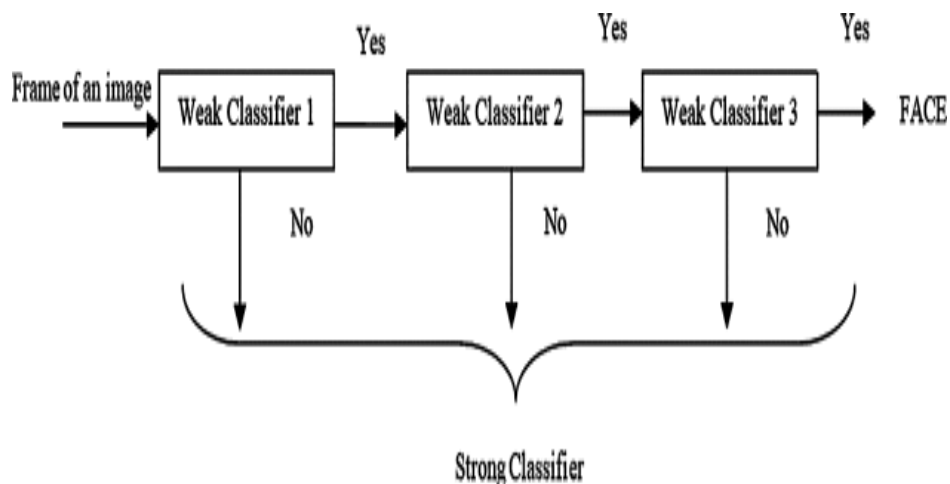
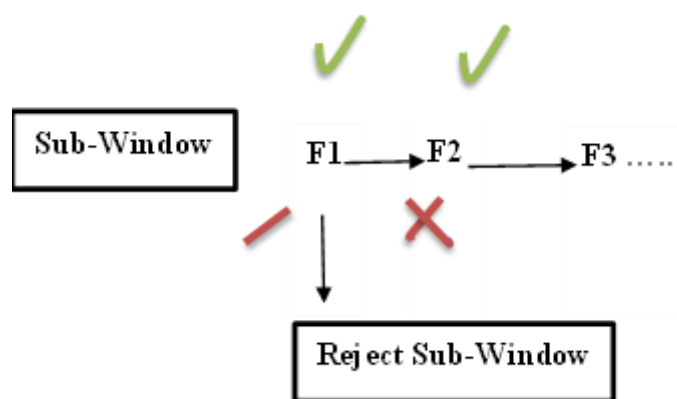


Figure III.10 Cascade classifier

Cascading is another sort of “hack” to boost the speed and accuracy of our model. So we start by taking a sub-window and within this sub-window, we take our most important or best feature and see if it is present in the image within the sub-window. If it is not in the sub-window, then we don’t even look at the sub-window, we just discard it. Then if it is present, we look at the second feature in the sub-window. If it isn’t present, then we reject the sub-window. We go on for the number of features have, and reject the sub-windows without the feature. Evaluations may take split seconds but since you have to do it for each feature, it could take a lot of time. Cascading speeds up this process a lot, and the machine is able to deliver results much faster. [36]

$$F(x) = a_1F_1(x) + a_2F_2(x) + a_3F_3(x) \dots \dots \quad \text{(CHAPTER III:.1)}$$



So just to add some closing remarks about the Viola-Jones Algorithm:

- ❖ The algorithm was developed in 2001 by Paul Viola and Michael Jones, the first of its kind, and was primarily used for facial detection applications.

- ❖ There are two steps to the algorithms: there's training with facial and non-facial images and then there's the actual detection.
- ❖ We have 2 steps for training: training the classifiers and Adaboost.
- ❖ We have 2 steps for detection: detecting the haar features and creating the integral image.
- ❖ Viola-Jones is one of the most powerful algorithms of its time and even though, there are better models out there today, Viola-Jones set the foundation for it in the field of facial detection.

III.3 Convolutional Neural Network (CNN)

III.3.1 Definition

A convolutional neural network (CNN) is a type of artificial neural network used in image recognition and processing that is specifically designed to process pixel data.

CNNs are powerful image processing, artificial intelligence (AI) that use deep learning to perform both generative and descriptive tasks, often using machine vision that includes image and video recognition, along with recommender systems and natural language processing. [38]

It is divided into two parts: features learning and classifications and that what will see in its architecture.

III.4 Conclusion

Viola-Jones is one of the most powerful algorithms of its time and even though, there are better models out there today, Viola-Jones set the foundation for it in the field of facial detection.

Convolution neural network has many methods and we touched on one of them, and we knew its architecture and how it works, and it is called Alex Net.

Alex Net is a work of supervised learning and got excellent results.

The Alex Net made revolutionary implementation on ConvNets that continues nowadays, such as ReLU.

It is not easy to have low classification errors without having overfitting.

CHAPTER IV: Application with GUI MATLAB

IV.1 Introduction

This chapter represents the most important step in the realization of our project and we will see at the end the test results of the performance of this system in a real environment. During this phase, we will present the material working environment and the development tools of our system.

IV.2 Working environment

We used:

- ❖ A laptop LENOVO used as a server with windows 7.
- ❖ Processor Intel ® Core ™ i5-4300u CPU.
- ❖ Installed Memory (RAM) 4 GO.

IV.3 Development Tools

IV.3.1 MATLAB 2020a

IV.3.1.1 General Presentation

MATLAB is both a calculation software and a high-level programming language. It is paid software, of which there are two free equivalents:

- ❖ Octave is software that uses the MATLAB language and can therefore use functions written in MATLAB. It is slower and a little less beautiful.
- ❖ SCILAB is developed by INRIA and the syntax differs a little from that of MATLAB but the spirit is the same. It is from my point of view still a little less practical than MATLAB.

MATLAB is a numerical calculation software, he can only solve numerical equations. The name MATLAB comes from Matrix Laboratory.

In MATLAB, objects are all matrices by default. A real variable is therefore seen by MATLAB as a 1×1 matrix. The product is therefore by default a matrix product. The type of the variables is not very important.

MATLAB can add a Boolean and a real, multiply an integer by a complex without problem. To launch MATLAB just run the MATLAB command in a terminal. This opens the main window of MATLAB. You can launch command lines directly there but most of the time you will go through the MATLAB editor which allows you to create scripts and functions.

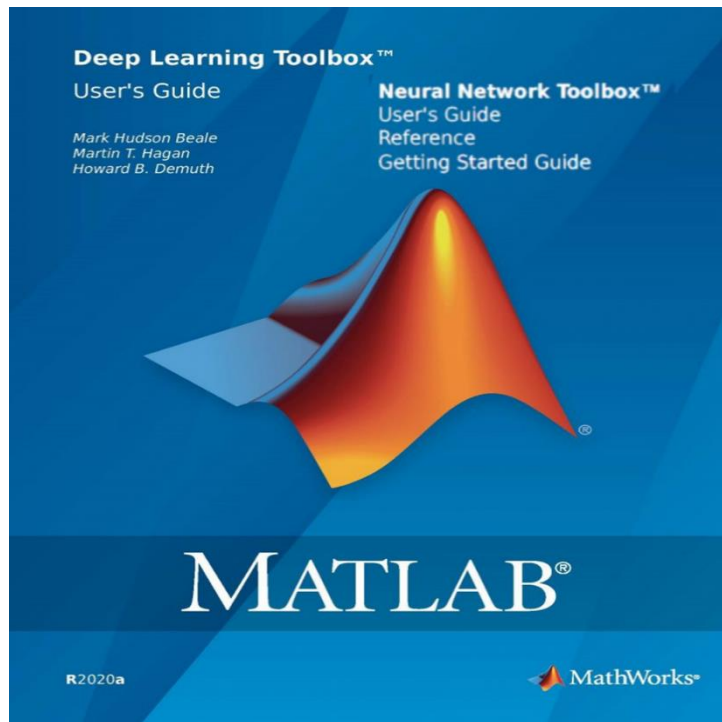


Figure IV.1 MATLAB 2020a

IV.3.1.2 The Peculiarities of MATLAB

MATLAB allows interactive work either in command mode or in programming mode, while still having the possibility of making graphic visualizations. Considered as one of the best programming languages (C or Fortran), MATLAB has the following particularities compared to these languages:

- ❖ Easy for programming
- ❖ continuity among integer, real, and complex values
- ❖ The extended range of numbers and their precision
- ❖ The very comprehensive mathematical library
- ❖ The GUI tool which includes GUI functions and utilities
- ❖ The possibility of linking with other classic programming languages (C or Fortran)

IV.3.1.3 Writing a MATLAB program

- ❖ In MATLAB programs end with '.m' extension in the program file name. No compilation is to be done before the execution of the program.
- ❖ During the execution, an error message appears and indicates the places where the errors are.
- ❖ To launch the execution of the program, you must always put yourself in the same directory where this program is located.

Example: the latter is located in c:\user; you must first change directory after launching MATLAB by typing: "cd c:\user" The data files are saved with '.mat' extension and the variables are saved twice

IV.3.1.4 Interests

- ❖ Infinitely faster programming for calculation and for display A very rich library.
- ❖ Possibility to include a C/C++ program.
- ❖ Interpreted language: No compilation so no waiting to compile
- ❖ Ability to run code outside of the program.
- ❖ Easy to understand and very readable code.
- ❖ A very well-done help.

IV.3.1.5 Disadvantages

- ❖ Calculation speed slower than in C/C++
- ❖ Inconvenient self-running app

Generally, MATLAB is used to do computational experiments very quickly. Some programs that would require 1 day of programming in C/C++ can be done in 1 hour in MATLAB. On the other hand, once programmed, the calculation time under MATLAB can be 100 times greater than that of C/C++. As a result, it is only used very little to produce a finished product intended for individuals.

IV.4 Overview of the Application

In this part we will detail the main steps and present the implementation of our application based on illustrations. The project is based on the following components:

IV.4.1 Graphic Interface Users

The interface consists of three parts that we will talk about in detail in this chapter.

The first part [creation new user] enables us to enter a new user name with click on [take picture] when we want to detect his face print.

While the second part [Machine learning], with a single click on [training],

Third part is authentication of the face and giving the person's name by recognizing his face. (Figure IV.2)

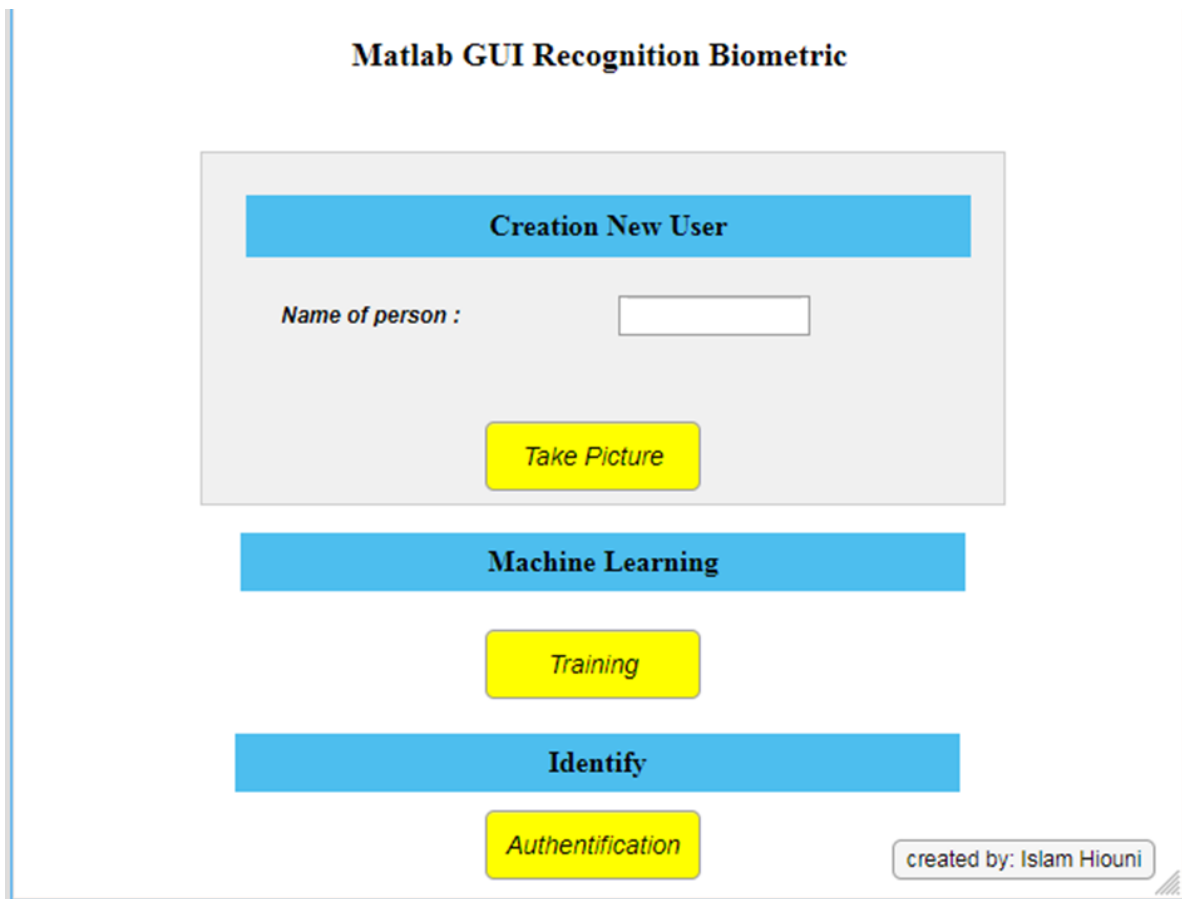


Figure IV.2 MATLAB GUI of Biometric Recognition

IV.4.2 Database

Database made up of 3 individuals, the database contains 20 pictures of each person, at a resolution of $(227*227*3)$ pixels, the images of the same person were taken at different times.

The database is created as follows:

- ❖ CLICK on the button take picture in the interface as shown in figure 4.2
- ❖ If the face is new and does not exist in database, the program creates a new file in the data base.

IV.4.3 Code of Application

To do what we speak previously about taking picture, create files in data base, training machine and identify persons we should follow this following step with codes that allow us to achieve our goal.

These three commands make it so past data is not linked with the new file.

- The command Close all; closes all open MATLAB figure windows.
- The command warning off; suppress all warning messages.
- The command Clc; clears the command window.

IV.4.3.1 Step 1: (Take Picture)

For open camera with button take picture we use main function:

Cam = webcam; // creates the webcam object cam and connects to the single webcam on your system

A webcam is a digital video device commonly built into a computer. Its main function popularly used with instant messaging services and for recording images.

First, we enter the user's name and click button take picture ():

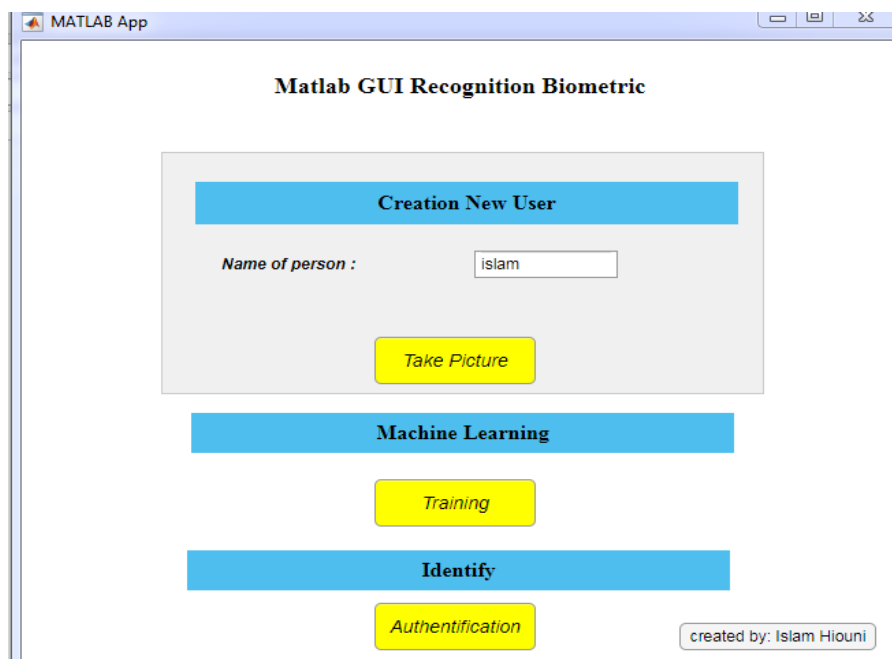


Figure IV.3 GUI after created user name

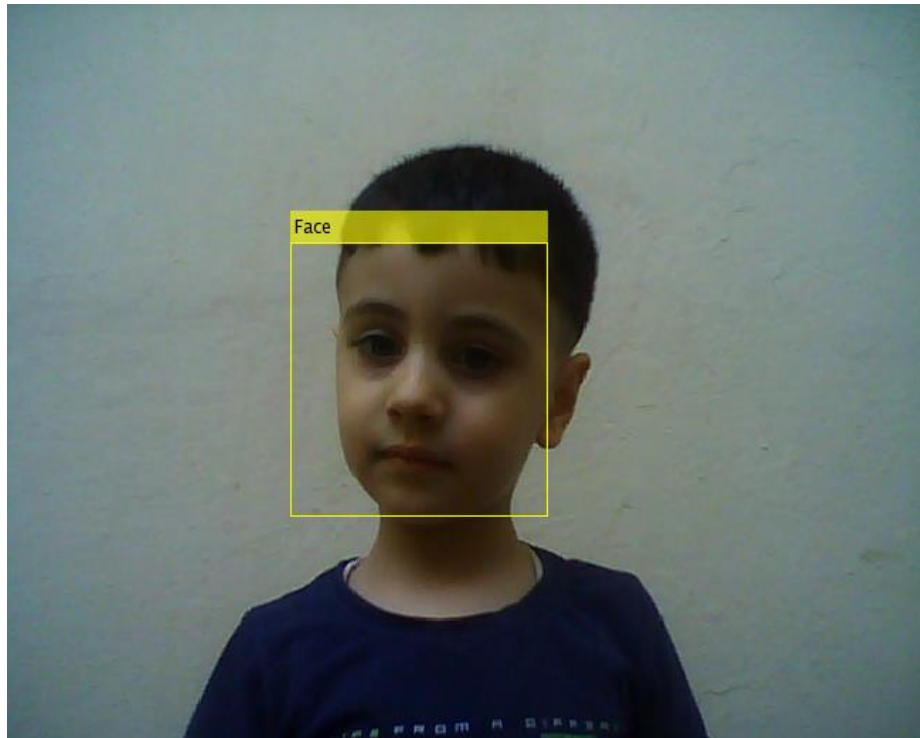


Figure IV.4 Face Detection

When we see these words ‘The operation has been successfully completed’: we can move to the next operation.

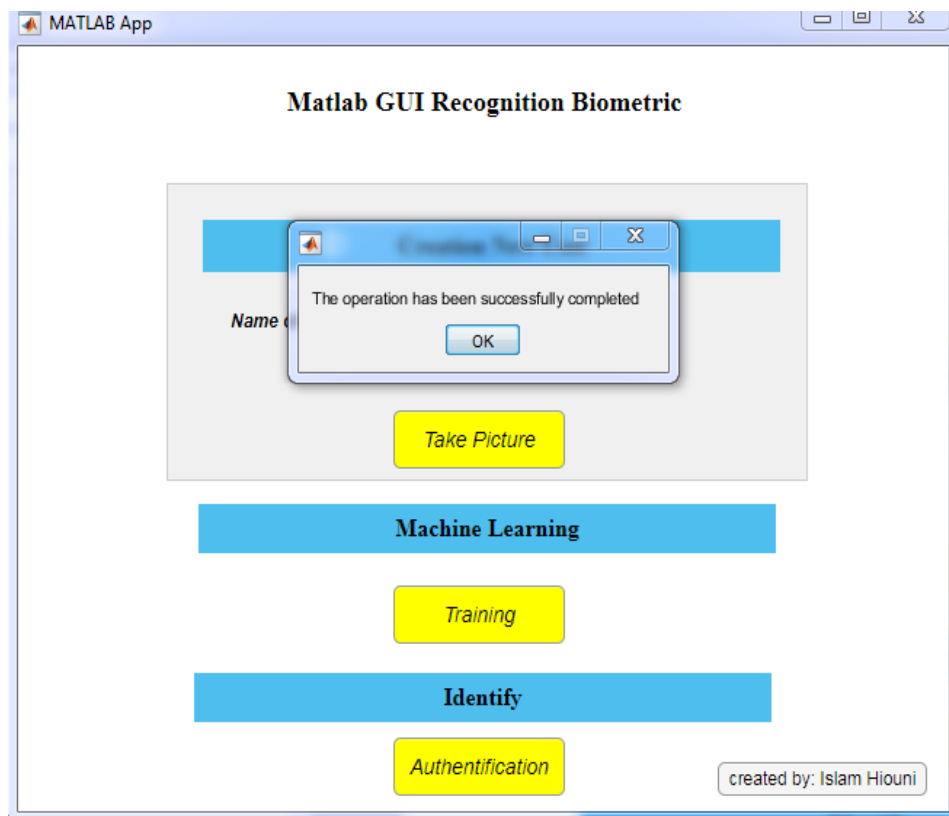


Figure IV.5 GUI Operation Completed

IV.4.3.2 Step 2: (Detect Face)

For detect face we use:

Face Detector = vision.CascadeObjectDetector; // creates a detector to detect objects using the Viola-Jones algorithm

Camera takes 20 photos or more (we can control this) and put them in folder in data base if exist if not create new folder with the new username in data base, after that we call cascade function of viola-jones algorithm to detect face and put it in its folder if exist if not then it is new user.

```
c=20;
temp=0;
nom = app.NompersonField.Value;
folder_name = [FOLDER_ROOT_NAME,sprintf(nom)];
if not(exist(folder_name,'dir'))
mkdir(folder_name)
end
```

after that we call cascade function mentioned in step 3 to detect face and put it in its folder if exist if not then it is new user.

```
folder_name = [folder_name , '\'];
while (temp<c)
e=cam.snapshot;
bboxes =step(faceDetector,e);
if(sum(sum(bboxes))~=0)
es=imcrop(e,bboxes(1,:));
filename=string(strcat(folder_name, num2str(temp), '.bmp'));
imwrite(es,filename);
temp=temp+1;
imshow(es);
drawnow;
else
imshow(e);
drawnow;
end
and to confirm that camera detect face;
msgbox("The operation has been successfully completed");
```

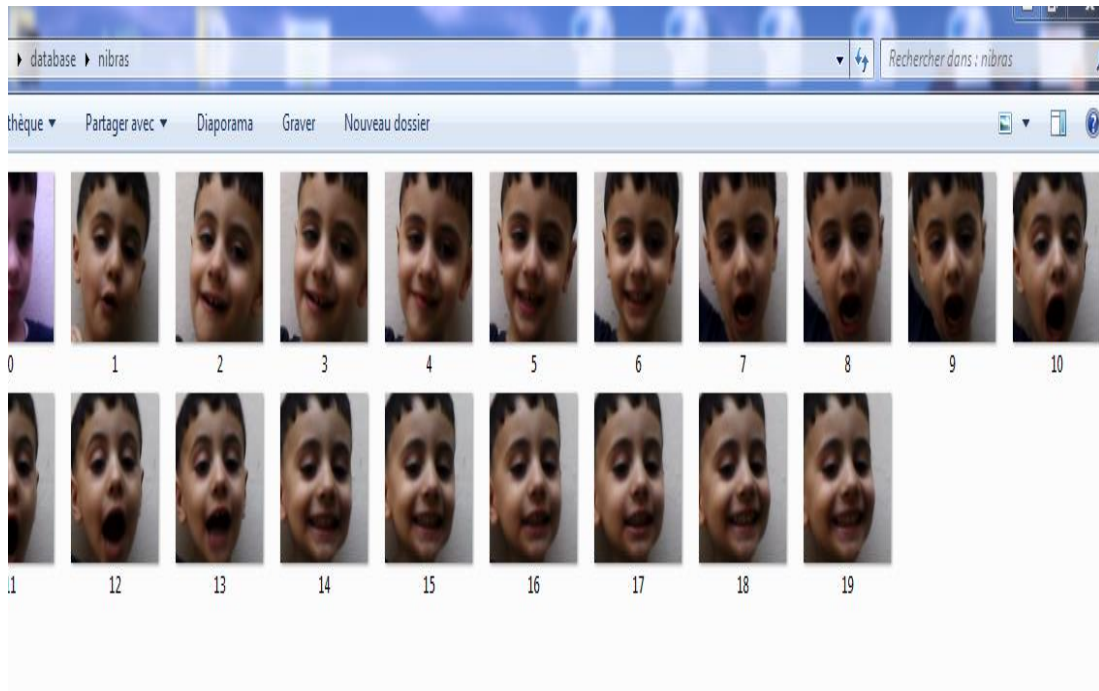


Figure IV.6 Database

IV.4.3.3 Step 3: (Training)

In the program we will just call training in its name but the program of training is:

```
function TrainingButtonPushed(app, event)
training;
msgbox("The operation has been successfully completed");
end

clc
close all
g=alexnet;
layers=g.Layers;
layers(23)=fullyConnectedLayer(3);
layers(25)=classificationLayer;
allImages=imageDatastore('database','IncludeSubfolders',true,
'LabelSource','foldernames');
opts=trainingOptions('sgdm','InitialLearnRate',0.001,'MaxEpochs',20,'Mini
BatchSize',64);
myNet=trainNetwork(allImages,layers,opts);
save myNet;
```

IV.4.3.4 Step 4: (authentication)

It's the same authentication it is a function we call it to program

```
% Button pushed function: AuthenticationButton
function AuthenticationButtonPushed(app, event)
comp;
end
% Create Authentication
incr = 0;
load myNet;
faceDetector=vision.CascadeObjectDetector;
while (incr<30)
e=c.snapshot;
bboxes =step(faceDetector,e);
if (sum(sum(bboxes))~=0)
    es=imcrop(e,bboxes(1,:));
    es=imresize(es,[227 227]);
    label=classify(myNet,es);
    image(e);
    incr = incr+1;
    title(char(label));
    drawnow;
else
    image(e);
    title('No Face Detected');
end
end
```

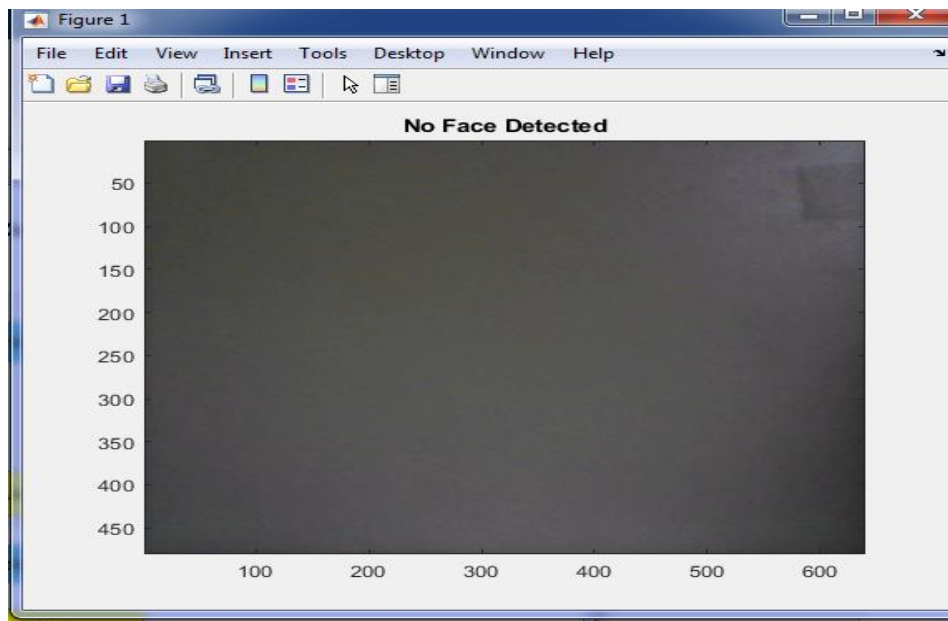


Figure IV.7 Camera no detected face

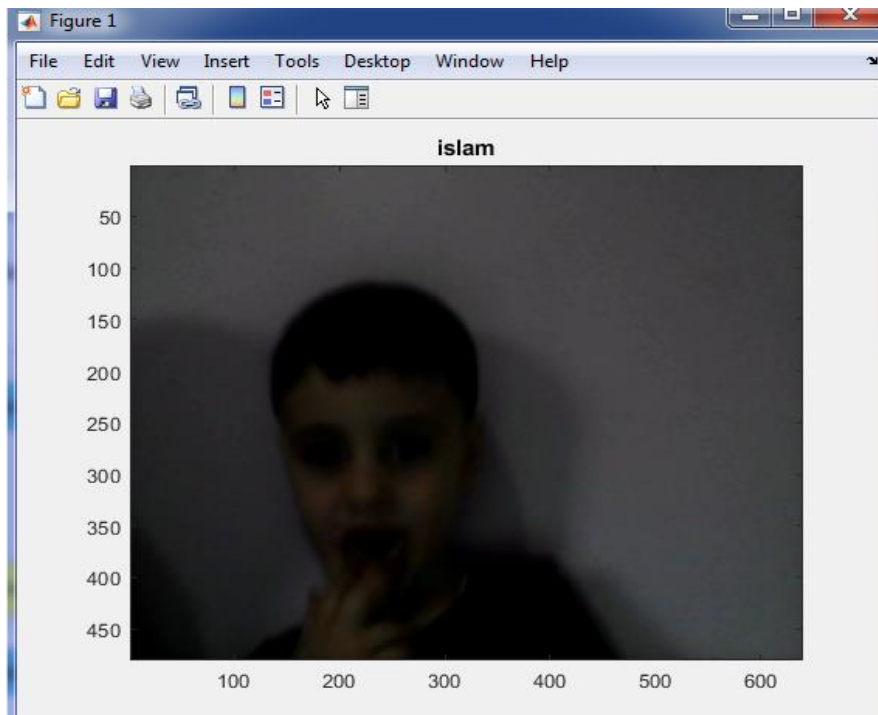


Figure IV.8 Authentication of new user

IV.5 Conclusion

At the end of this chapter, we obtain an almost complete view of our application from the design side. And we explained the efficiency of the system by submitting various experiments on a powerful test environment. The results we have obtained are encouraging.

GENERAL CONCLUSION

In this manuscript, we presented a survey on biometrics identity, its types and its importance in what the world has reached today. It is considered the most advanced protection and identification tool ever. Therefore, our world today and until now continues to research and develop in the hope of making maximum use of this modern technological field.

Facial recognition is one of the most important types of biometrics, if not the most important and best currently. We knew how it started and where it came from development, and due to this, it reduced joint profits to its discoverers and developers, as well as its workers, and we were able to work on it by following the methodology of the two scientists, Viola and Jones, and we concluded the extent of its value and impact on the life of even the ordinary person from facilitating tasks and taking technology to another world.

As we wrote for our work in the introduction, here we come to our conclusion by achieving all the desired goals of this work. Each chapter was more important than the other, and each one carried a large amount of valuable information, some of which we quoted from books and scientific articles, and others we deduced, as well as without forgetting our work and our diligence, which It was clearly shown in the fourth chapter and the practical results.

The MATLAB program has given us a lot and is still being offered until now and helped us in terms of library of its offices, which saved us a great effort

We relied on the database, on which the computer depends in learning and training in order to know the identity of the person and for Detection face, and this is what we succeeded in presenting. The larger the database, the faster the training for the computer, and the greater its success rate in recognition.

In the end, the face technology is constantly evolving to the point of making the most of it by reaching the largest possible of database.

BIBLIOGRAPHY

- [1] Chandra, E.Kanagalakshmi, K. Cancelable biometric template generation and protection schemes: A review. (2011) *Electro Comput Tech-nol*
- [2] David Maltoni Biometric Systems laboratory -DEIS- University of Bologna via Sacchi 3, 47023, Cesena – Italy.
- [3] J. Daugman, Biometric Personal Identification System Based on Iris Analysis, United States Patent.
- [4] J. Daugman, “Statistical Richness of Visual Phase Information: Update on Recognizing Persons by Iris Patterns,” *Int’l J. Computer Vision*, vol. 45, no.1, pp. 25- 38, 2001.
- [5] J. Daugman, “Demodulation by Complex-Valued Wavelets for Stochastic Pattern Recognition,” *Int J. Wavelets, Multi resolution and Information Processing*, vol.1, no.1, pp.1-17, 2003.
- [6] J. Daugman, “How Iris Recognition Works”, University of Cambridge, 2001.
- [7] Scott T Smith Dog ear publishing, 2006.
- [8] Mohamad El Abed, Christophe Charrier, Evaluation of Biometric Systems, *New Trends and Developments in Biometrics*, pp. 149 - 169, 2012.
- [9] Odile PAPINI ESIL, Coures 06 "Biométrie" Université de la méditerranée.
- [10] PFPDT, Tour d’horizon des technologies biométriques Projet CCT, juin 2012.
- [11] www.securiteinfo.com consulté le 10/02/2017.
- [12] G.Ababsa Souhila, Authentication D’individus Par Reconnaissance De Caractéristiques Biométriques Liées Aux Visages 2d/3d, Thèse Pour Obtenir Le Titre De Docteur De L’université Evry Val D’Essonne Spécialité: Sciences De L’ingénieur, 03 octobre 2008.
- [13] [https://www.tutorialspoint.com/biometric/ biometric-modalities](https://www.tutorialspoint.com/biometric/biometric-modalities).

- [14] www.biometricsinstitute.org/types-of-biometrics-dna.
- [15] Arun, A. R., Anil, K. J., and Patrick, J. F. (2008). Handbook of biometrics. New York, NY: Springer.)
- [16] Arun, Anil, and Patrick, 2008, p. 12
- [17] W. W. Bledsoe, 'The model method in facial recognition', Panoramic Res, Inc, Palo Alto, CA, USA, Tech. Rep. PRI:15, 1964.
- [18] The International Journal of Mathematics, Science, Technology and Management (ISSN : 2319-8125) Vol. 2 Issue 3
- [19] John D. Woodward, Jr., Christopher Horn, Julius Gatune, and Aryn Thomas, 'Biometrics A Look at Facial Recognition' Prepared for the Virginia State Crime Commission.
- [20] web cite : <https://www.kaspersky.com/resource-center/definitions/what-is-facial-recognition>.
- [21] J.WPeirceA.ELeighK.MKendrick 'Configurational coding, familiarity and the right hemisphere advantage for face recognition in sheep' Laboratory of Cognitive and Developmental Neuroscience, Babraham Institute, Babraham, Cambridge CB2 4AT, UK.
- [22] RhodesG.Configural Coding, Expertise, and the Right Hemisphere Advantage for Face Recognition Univ Canterbury, Dept Psychol, Christchurch 1, New Zealand.
- [23] Sharif M., Mohsin S. and Javed M. Y., "A Survey: Face Recognition Techniques", Research Journal of Applied Sciences, 4, (2012).
- [24] http://en.wikipedia.org/wiki/Eigenvalues_and_eigenvectors [Last Visited: 10th April 2015]
- [25] Slavković, Marijeta, and DubravkaJevtić. "Face recognition using eigenface approach." Serbian Journal of electrical engineering 9.1 (2012): 121-130.
- [26] Gupta, Bhaskar, Sushant Gupta, and Arun Kumar Tiwari. "Face Detection Using Gabor Feature Extraction and Artificial Neural Network." Proceedings from IS CET (2010): 18-23.
- [27] Jin, Yi, and Qiu Qi Ruan. "Face recognition using gabor-based improved supervised locality preserving projections." Computing and Informatics 28.1 (2012): 81-95.
- [28] Bellakhdhar, Faten, Kais Loukil, and Mohamed Abid. "Face recognition approach using Gabor Wavelets, PCA and SVM." IJCSI International Journal of Computer Science Issues 10.2 (2013): 201-206.

- [29] Kar, Arindam, et al. "Classification of high-energized gabor responses using bayesian PCA for.
- [30] Muhammad Sharif1 , Farah Naz1 , Mussarat Yasmin1 , Muhammad Alyas Shahid1 and Amjad Rehman2 1 Department of Computer Science, Comsats Institute of Information technology WahCantt 2 MIS Department CBA Salman bin Abdulaziz University Alkharj KSA Received 6 January 2017; Accepted 12 March 2017.
- [31] D. Abdullah, Tulus, S. Suwilo, S. Effendi, and Hartono, "DEA Optimization with Neural Network in Benchmarking Process," IOP Conf. Ser. Mater. Sci. Eng., vol. 288, no. 1, p. 012041, 2018.
- [32] S. Zafeiriou, C. Zhang, and Z. Zhang, "A survey on face detection in the wild: Past, present and future," Comput. Vis. Image Underst., vol. 138, pp. 1–24, Sep. 2015.
- [33] C. Holzmann and M. Hochgatterer, "Measuring Distance with Mobile Phones Using SingleCamera Stereo Vision," 2012, pp. 88–93.
- [34] R. Belaroussi and M. Milgram, "A comparative study on face detection and tracking algorithms," Expert Syst. Appl., vol. 39, no. 8, pp. 7158–7164, Jun. 2012.
- [35] Z. Zakaria, S. A. Suandi, and J. Mohamad-Saleh, "Hierarchical Skin-AdaBoost-Neural Network.
- [36] Breaking Down Facial Recognition: The Viola-Jones Algorithm
<https://towardsdatascience.com/the-intuition-behind-facial-detection-the-viola-jones-algorithm-29d9106b6999>.
- [37] Face Detection using Viola Jones Algorithm.
<https://www.mygreatlearning.com/blog/viola-jones-algorithm/>