INTERNATIONAL JOURNAL OF SCIENTIFIC RESEARCH AND INNOVATIVE STUDIES
ISSN: 2820-7157
www.ijsrisjournal.com

February 2025 Volume 5 Number 1 70-89

Received Date: December 20, 2025 Accepted Date: January 12, 2026 Published Date: February 01, 2026

Implementation of a biometric system for automatic control

KAPALALA KAPENDA Blaise [1], KINDUKULU LUBOKO Rucien [2], ETUMANGELE TSHITAKA Gabriel [3], LUKOKI TULANDA Dan [4]

1. PhD Student – Higher Institute of Education – Gombe Kinshasa– DRC, online: (+212) 612-975163, (+243) 211459397, blaisekapalala94@gmail.com
2. Higher Institute of Education – Gombe Kinshasa – DRC, online: (+243) 816 888 654, kindukulurucien@gmail.com
3. Higher Institute of Education – Gombe Kinshasa – DRC, online: (+243) 817 851 599, gabrieletums2015@gmail.com
4. Higher Institute of Education – Gombe Kinshasa – DRC, online: (+243) 823 841 178, danlukoki2@gmail.com

Abstract

With the rapid development of digital technologies and increasing security requirements, traditional access control systems based on passwords, cards, or PIN codes show significant limitations. Biometrics, which relies on identifying individuals through unique physiological or behavioural characteristics, has emerged as a reliable and efficient solution. This paper presents the implementation of a biometric system for automatic access control. It discusses the theoretical foundations of biometrics, existing technologies, system architecture, design and implementation stages, as well as technical, ethical, and security challenges.

Keywords: Biometrics, automatic control, security, recognition, information systems.

Introduction

The security of people, property and information is now a major challenge for public and private organisations. Traditional access control systems, such as badges, keys or passwords, are vulnerable to loss, theft, duplication or forgetfulness. These weaknesses have led to the emergence of more robust solutions based on biometrics. Biometrics relies on the use of characteristics specific to each individual, such as fingerprints, facial features, iris patterns, voice patterns, and even gait patterns. Thanks to these unique characteristics, biometric systems offer a higher level of security and enable fast and reliable automatic control.

This article aims to present a comprehensive approach to implementing a biometric system for automatic control, from theoretical concepts to practical aspects of implementation. The rapid evolution of information and communication technologies has profoundly transformed the ways in which modern organisations are managed, secured and controlled. In a context marked by increasing flows of people, the dematerialisation of services and the proliferation of security threats, the implementation of reliable and automated control mechanisms has become an essential requirement.

In this context, this article aims to study the implementation of a biometric system for automatic control, highlighting the fundamental principles of biometrics, existing technologies and the stages of design and implementation of such a system. The aim is to analyse the advantages and limitations of biometric solutions, while highlighting their contribution to improving the security and efficiency of control systems. This study also seeks to identify opportunities for development and innovation, particularly through the integration of artificial intelligence and emerging technologies, in order to meet current and future security challenges.

1. General information on biometrics

1.1 Definition of biometrics

Biometrics is the science of identifying and authenticating individuals based on measurable and unique biological or behavioural characteristics. Biometrics is a scientific and technological discipline concerned with the identification and authentication of individuals based on characteristics specific to each person. These characteristics, known as biometric traits, can be physiological or behavioural. Unlike traditional identification methods based on what an individual possesses (card, badge, key) or knows (password, secret code), biometrics is based on what an individual is. This approach gives biometric systems a significant advantage in terms of security, reliability and ease of use.

Conceptually, biometrics can be defined as the set of techniques used to automatically recognise a person based on their measurable biological or behavioural characteristics. These characteristics must be unique or sufficiently distinctive to differentiate one individual from another within a given population. This uniqueness is the very foundation of biometrics and justifies its use in automatic control and security systems.

Historically, the use of physical characteristics to identify individuals did not begin in the digital age. Since ancient times, certain societies have used bodily marks or fingerprints to recognise people. However, it was at the end of the 19th century that modern biometrics truly emerged with the introduction of fingerprint recognition in judicial and police systems. Advances in computer technology and signal processing algorithms then enabled the automation and widespread use of biometric systems.

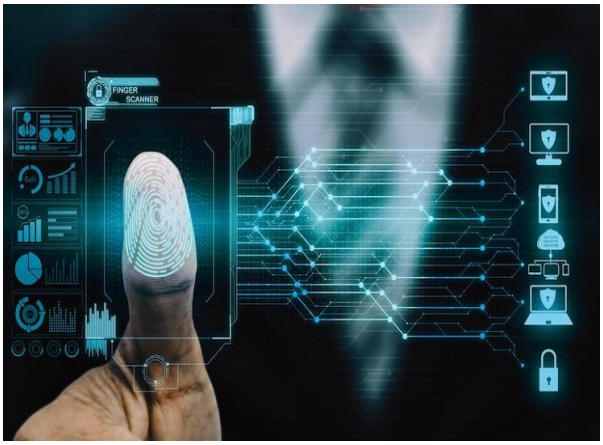


Figure 1: Biometric system

1.2 Types of biometrics

There are two main categories:

- **Physiological biometrics**: fingerprints, face, iris, retina, DNA.
- **Behavioural biometrics**: voice, signature, keystroke, gait.

1.2.1 Physiological biometrics

Physiological biometrics is based on the analysis of the physical and biological characteristics of the human body, which are intrinsic to each individual and relatively stable over time. These characteristics are reliable identification elements that are widely used in automatic control and security systems. Among the most common physiological biometric technologies are fingerprint recognition, facial recognition, iris recognition, retina analysis and DNA identification. Each of these methods has specific advantages, limitations and areas of application.

Figure 2: Physiological biometrics

Figure 3: Fingerprint

1. Fingerprint recognition

Fingerprint recognition is one of the oldest and most widely used biometric technologies. It is based on the analysis of patterns formed by ridges and valleys on the surface of the fingers. These patterns, known as minutiae, include bifurcations, endings and islands, which are unique to each individual, even twins. The fingerprint recognition process begins with the capture of the fingerprint using an optical, capacitive or ultrasonic sensor. The image obtained is then pre-processed to improve its quality, and distinctive features are extracted and stored as a biometric template.

During authentication, the fingerprint provided is compared to the stored template to determine a match. This technology is widely used because of its relatively low cost, ease of integration and good level of accuracy. It is commonly used in access control systems, attendance management, smartphones and public security devices. However, fingerprint recognition can be affected by skin condition, injuries, or wear and tear on the fingers, which can lead to recognition errors.

2. Facial recognition

Facial recognition is based on the analysis of facial features, such as the distance between the eyes, the shape of the nose, the structure of the jaw and the texture of the skin. Unlike fingerprint recognition, this method allows for contactless identification, making it particularly suitable for environments requiring rapid and hygienic interaction. The facial recognition system captures an image or video sequence of the face using a camera, then applies image processing and artificial intelligence algorithms to extract facial features. These features are then compared to those stored in the database to identify or verify the individual. Thanks to recent advances in deep learning, facial recognition has seen significant improvements in terms of accuracy and robustness.

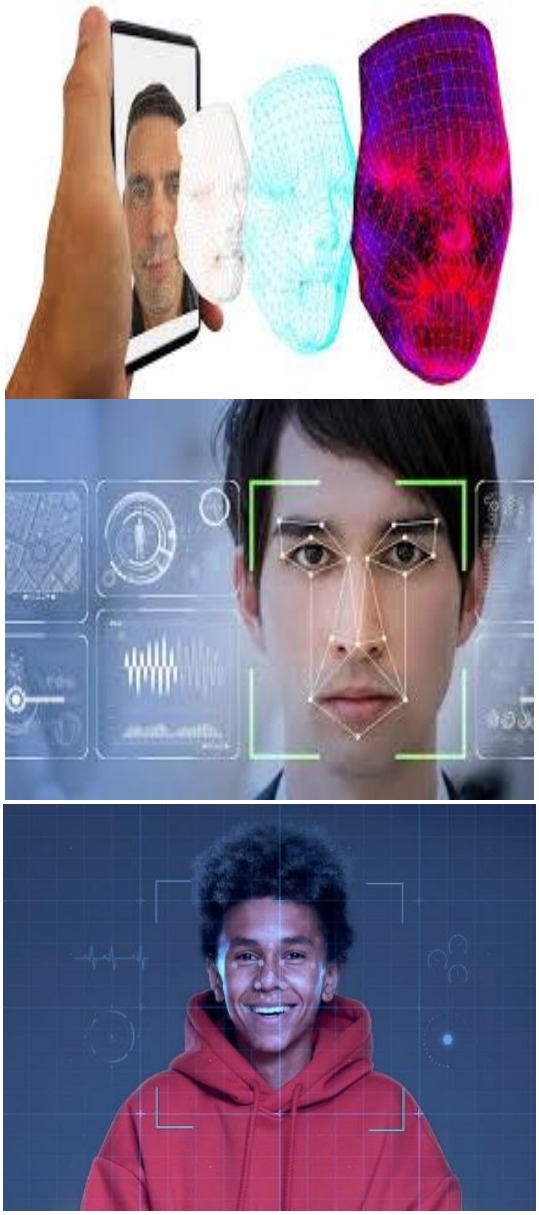


Figure 4: Facial recognition

3. Iris recognition

Iris recognition is based on the analysis of complex and unique patterns in the iris, the coloured part of the eye. These patterns are extremely distinctive and remain stable throughout a person's lifetime, giving this technology a very high level of accuracy. The iris recognition process involves capturing an image of the eye using a specialised camera, often equipped with infrared lighting.

The iris patterns are then extracted and encoded as a biometric template. During verification, the extracted template is compared to the patterns stored in the database. Iris recognition is considered one of the most reliable biometric technologies, with very low error rates. It is used in applications requiring a high level of security, such as sensitive access controls and government security systems. However, its high cost and the need for specialised equipment sometimes limit its widespread adoption.

Offers very high accuracy but requires expensive equipment. Iris recognition is a biometric technique based on the analysis of unique patterns in the iris of the human eye. The iris, the coloured membrane between the cornea and the pupil, has complex patterns that form before birth and remain largely stable throughout life. These patterns, including streaks, rings, crypts and pigment spots, are highly distinctive and make iris recognition one of the most reliable biometric methods.

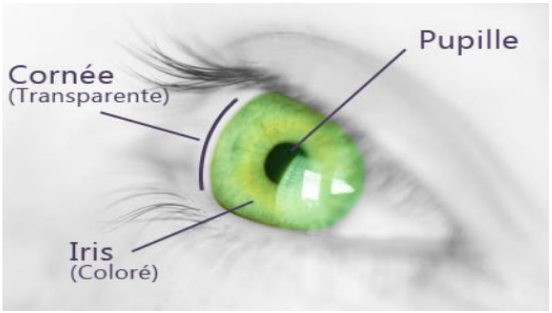


Figure 5: Iris recognition

4. Retinal analysis

Retinal analysis is a biometric method based on examining the blood vessels at the back of the eye. The arrangement of these vessels is unique to each individual and offers an exceptional level of accuracy. Capturing an image of the retina requires a specialised optical device and active cooperation from the user, who must stare at a specific point during acquisition. This constraint makes the technology less user-friendly than other biometric methods. Although retinal analysis offers a very high level of security, its intrusive nature, high cost and complexity of use limit its deployment to very specific environments, such as high-security facilities.

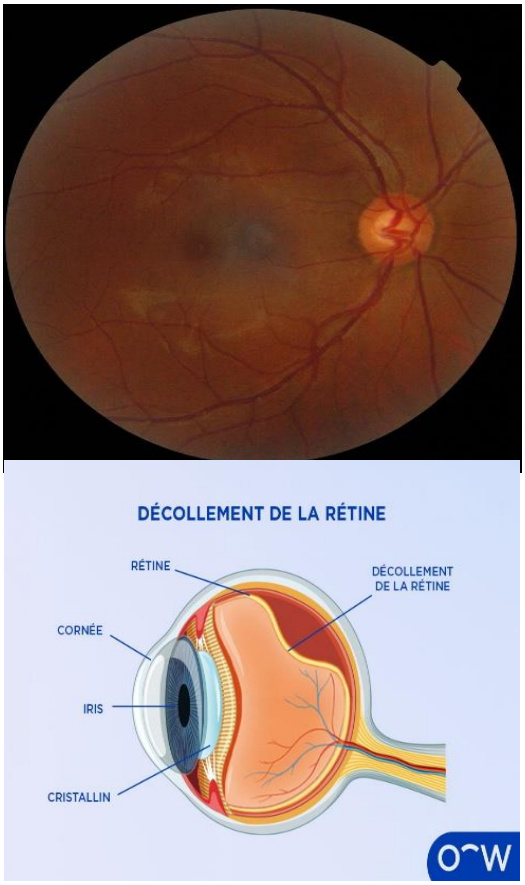


Figure 6: Retinal scanning

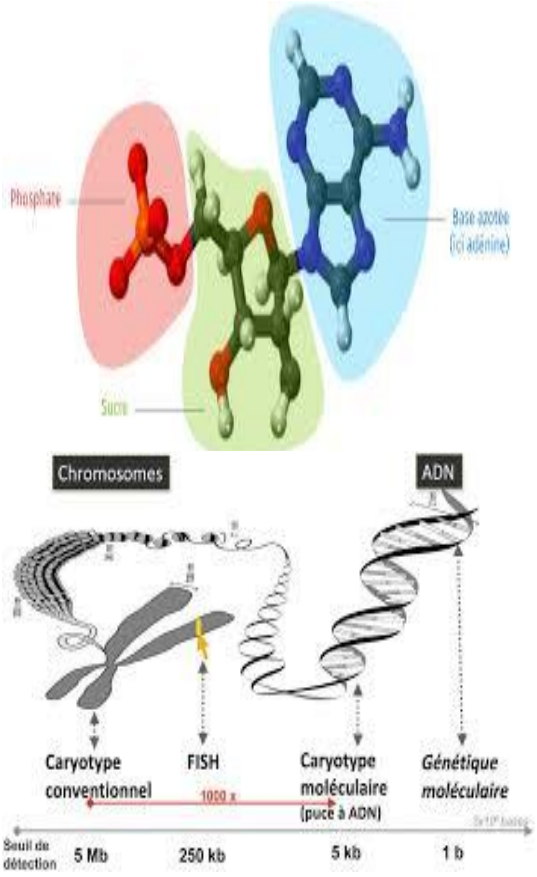


Figure 7: DNA identification

5. DNA identification

DNA identification is based on the analysis of genetic material contained in human cells. DNA is considered the most accurate biometric characteristic because it is unique to each individual, with the exception of monozygotic twins. This method requires the collection of a biological sample, such as blood, saliva or hair, followed by laboratory analysis.

Due to the complexity of the process and the time required for analysis, DNA identification is not generally used for automatic real-time monitoring. DNA is mainly used in the fields of forensics, judicial identification and scientific research. Its use raises major ethical and legal issues, particularly with regard to the protection of genetic data and privacy.

1.2.2 Behavioural biometrics

Behavioural biometrics is based on the analysis of behaviours specific to each individual rather than fixed physical characteristics. It relies on behavioural patterns acquired and developed over time, such as the way a person speaks, writes, types or moves. Unlike physiological biometrics, these characteristics can be influenced by psychological, environmental or contextual factors.

However, when properly modelled and analysed, they offer an effective means of identifying and authenticating individuals, particularly in digital environments. Behavioural biometrics technologies are particularly valued for their less intrusive nature and their ability to operate continuously and transparently for the user. They are often used in conjunction with physiological methods to enhance the overall security of biometric systems.

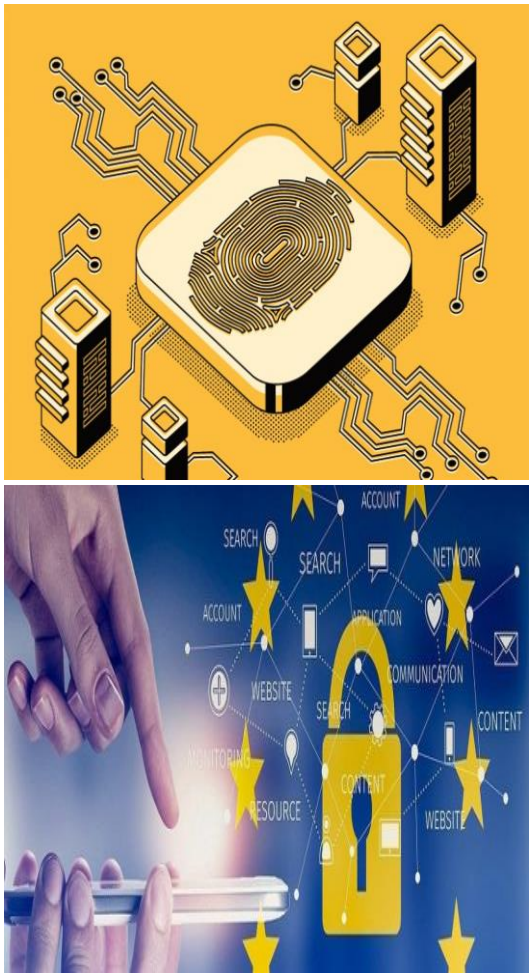


Figure 8: Behavioural biometrics

A. Voice recognition

Voice recognition is based on the analysis of the acoustic characteristics of the human voice. Each individual has a unique voice resulting from the configuration of their vocal apparatus, including the vocal cords, oral cavity and respiratory tract. In voice biometrics, the system analyses parameters such as fundamental frequency, timbre, intonation, speech rate and formants. The voice recognition process begins with the capture of the audio signal using a microphone.

B. Handwriting recognition

Handwritten signature recognition is a biometric method based on analysing the way a person signs their name. It is not limited to the visual aspect of the signature, but also takes into account dynamic parameters such as writing speed, pressure exerted on the medium, acceleration and the order of strokes. This technology can be implemented statically, using an image of the signature, or dynamically, using graphics tablets or digital devices capable of capturing temporal parameters.

Dynamic recognition is generally more reliable, as it incorporates behavioural information that is difficult to reproduce. Signature biometrics is widely used in the banking, legal and administration, where signatures remain a recognised means of authentication. However, this method can be influenced by emotional state, fatigue or writing conditions, which can lead to variability in system performance.

Figure 9: Handwritten signature recognition

C. Keyboard typing dynamics

Keyboard typing dynamics biometrics analyses the way an individual types on a keyboard. Each person has a unique typing rhythm, characterised by parameters such as the time spent pressing a key, the interval between keystrokes and typing speed. The main advantage of this technology is that it does not require any additional hardware, as it can be implemented on existing computer systems.

It enables continuous authentication, meaning that the user's identity can be verified at all times while using the system. Typing biometrics is particularly well suited to digital environments and computer access control systems. However, it can be affected by factors such as stress, fatigue, the use of different keyboards, or changes in posture, which requires mechanisms for adapting biometric models.

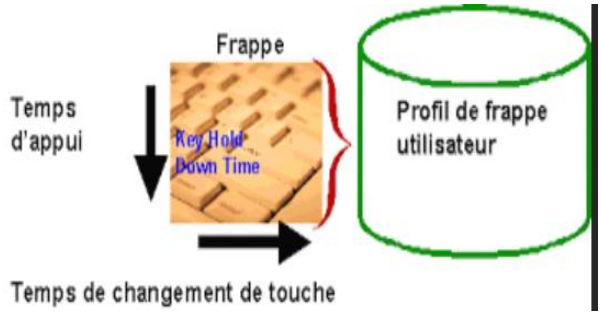


Figure 10: Keyboard typing

D. Gait recognition

Gait recognition is based on analysing the way a person moves. Human gait is influenced by body structure, muscle coordination and movement habits, making it relatively distinctive. This technology uses video sensors or inertial sensors to capture body movements, then applies signal processing and computer vision algorithms to extract gait characteristics.

Gait recognition has the advantage of being able to identify individuals from a distance, without contact or active cooperation. It is mainly used in surveillance and public security systems. However, gait can be altered by factors such as carrying loads, clothing, injuries or terrain conditions, which can affect the accuracy of the system.

Figure 11: Gait recognition

1.3 Criteria for a biometric characteristic

A biometric characteristic refers to a measurable attribute of an individual that allows them to be reliably identified or authenticated. However, not all human characteristics can be effectively exploited in a biometric system. To be considered relevant and exploitable, a biometric characteristic must meet a set of fundamental criteria that are generally recognised in scientific literature. A biometric characteristic must be:

- Universal,
- Unique,
- Permanent,
- Measurable,
- Acceptable to users.

1. **Universality:** Universality means that every individual in the relevant population must possess the biometric characteristic in question. An effective biometric system must be capable of identifying all users without exception. For example, fingerprints are largely universal, although some people may have altered fingerprints due to injury, illness or intensive manual labour.

The lack of universality can limit the applicability of a biometric system and require the integration of alternative methods. Thus, in critical environments, multimodal systems are often preferred in order to overcome the limitations associated with the universality of a single biometric characteristic.

2. **Uniqueness:** Uniqueness refers to the ability of a biometric characteristic to reliably distinguish between two different individuals. The more unique a characteristic is, the more accurate the identification and the lower the risk of confusion between users. For example, DNA has an extremely high level of uniqueness, whereas voices or signatures may show similarities between certain individuals. Uniqueness is a key criterion in large-scale identification systems, where the number of users is high. Low uniqueness can increase false acceptance rates, compromising the overall security of the biometric system.

3. **Permanence (or stability):** Permanence refers to the stability of the biometric characteristic over time. A good biometric characteristic should remain relatively unchanged throughout an individual's lifetime. Fingerprints, irises and DNA have excellent permanence, while voice, signature or gait can vary depending on age, health or emotional state. Low permanence requires regular updating of biometric templates in order to maintain satisfactory performance. This adds complexity to the management of

biometric systems and can affect their long-term reliability.

4. **Measurability (or collectability):** Measurability refers to the ease with which a biometric characteristic can be captured, measured and digitised using technical devices. A biometric characteristic must be easily exploitable by available and affordable sensors, while ensuring sufficient quality of the data collected. For example, facial recognition benefits from widely available sensors such as digital cameras, while iris or DNA analysis requires more specialised and expensive equipment. Good measurability promotes the widespread adoption of biometric systems.

5. **Performance:** The performance of a biometric characteristic is assessed using indicators such as false acceptance rate (FAR), false rejection rate (FRR) and equal error rate (EER). A high-performance biometric characteristic must offer a good compromise between security and user-friendliness. Performance also depends on the algorithms used, the quality of the sensors and the conditions of use. A biometric characteristic may be intrinsically reliable, but perform poorly if the capture conditions are not controlled.

2. How a biometric system works

A biometric system is a technological device that enables the automatic identification or authentication of an individual based on their biological or behavioural characteristics. It operates on the basis of a well-defined chain of processes, from the capture of biometric data to the final decision. The reliability and effectiveness of a biometric system depend on the quality of each of these steps and their consistent integration. A biometric system is based on two main phases:

- **enrolment**, which consists of capturing and recording biometric data;
- **recognition**, which allows an individual to be identified or verified.

The process includes:

1. Acquisition of the biometric signal;
2. Pre-processing;
3. Feature extraction;
4. Comparison with the database;

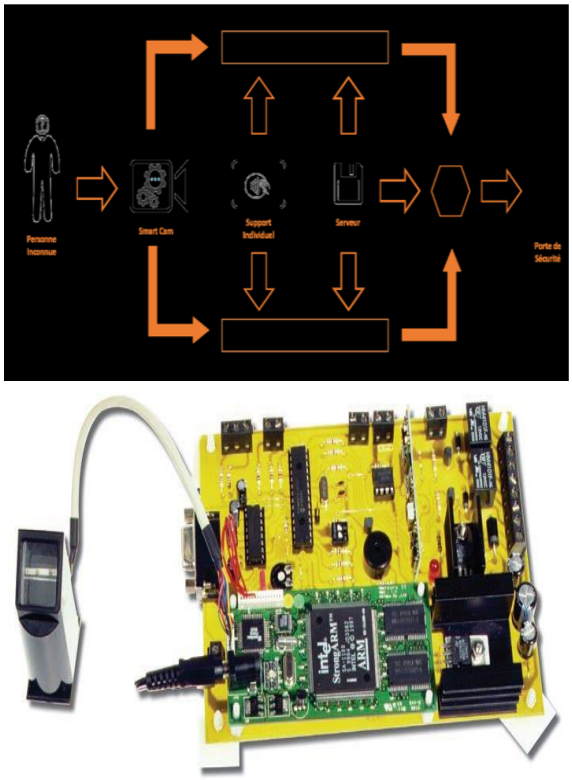


Figure 12: How a biometric system works

2.1 Acquisition of biometric data

The first step in the operation of a biometric system is the acquisition of biometric characteristics using an appropriate sensor. This sensor may be a camera for facial recognition, an optical or capacitive reader for fingerprints, a microphone for voice recognition, or an infrared sensor for iris analysis. The quality of the acquisition is a determining factor, as poorly captured data can lead to errors throughout the process. Elements such as lighting, user position, the physical condition of the characteristic (dirt, injuries, fatigue) and environmental conditions directly influence the quality of the biometric data collected.

2.2 Data pre-processing

Once the biometric data has been acquired, it undergoes a pre-processing phase to improve its quality and reduce interference. This step generally includes noise removal, data normalisation, contrast enhancement, and segmentation of the area of interest. For example, in the case of fingerprints, pre-processing enhances ridges and valleys to facilitate the extraction of minutiae.

2.3 Feature extraction

Feature extraction is at the heart of the biometric system. It consists of transforming raw biometric data into a set of discriminating parameters, called a "biometric template." These features must be compact, unique, and stable over time. Extraction techniques vary depending on the type of biometrics. For fingerprints, these are generally minutiae (endings and bifurcations of ridges).

2.4 Security and protection of biometric data

Throughout the process, the security of biometric data must be guaranteed. Biometric templates must be protected against unauthorised access using encryption, hashing and access control techniques. Unlike passwords, biometric data cannot be changed if compromised, which reinforces the importance of protecting it. Modern systems also incorporate liveness detection mechanisms to prevent impersonation attacks. These devices verify that the biometric characteristic comes from a living individual and not an artefact.

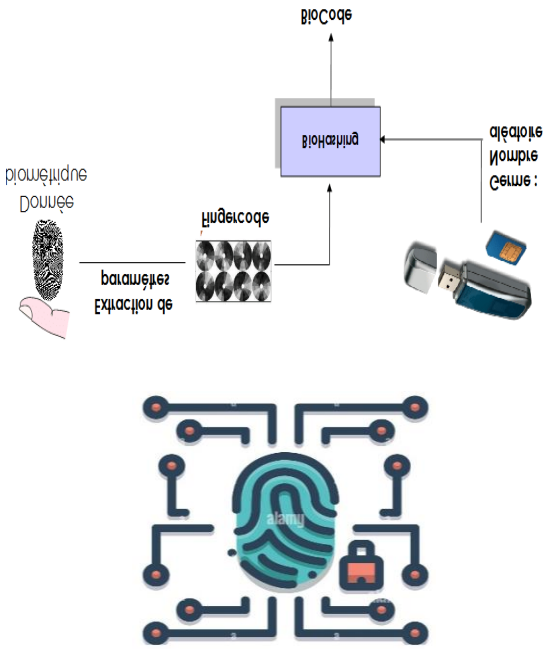


Figure 13: Biometric data security

3. Biometric technologies used in automatic control

3.1 Fingerprint recognition

This is the most widely used technology, valued for its reliability and low cost. Fingerprint recognition is one of the oldest, most widespread and most reliable biometric techniques used for identifying and authenticating individuals. It is based on analysing the unique patterns formed by the ridges and valleys on the surface of the fingers. These patterns, which appear at birth and remain largely stable throughout life, give fingerprints a highly distinctive character.

3.1.1 General principles of fingerprint recognition

The fundamental principle of fingerprint recognition is to compare an acquired fingerprint with a set of fingerprints previously stored in a database. This comparison is based on the extraction and analysis of specific characteristics called minutiae, which mainly correspond to the endings and bifurcations of the papillary ridges. Each individual has unique fingerprints, even between the fingers of the same hand. This uniqueness makes fingerprints a reliable means of personal identification, particularly in access control, attendance management and secure authentication systems.

3.1.2 Fingerprint acquisition

Fingerprint acquisition is the first step in the recognition process. It is performed using specialised sensors, which can be optical, capacitive, thermal or ultrasonic. These sensors capture the image of the fingerprint by detecting the differences in relief between the ridges and valleys. The quality of the image acquired depends on several factors, including the cleanliness of the finger, the pressure exerted on the sensor, the condition of the skin and environmental conditions. Quality control mechanisms are often built in to reject blurred or incomplete images, thus ensuring the reliability of the system.

3.1.3 Pre-processing and feature extraction

Once the fingerprint image has been acquired, it undergoes a series of processes to improve its quality. Pre-processing generally includes noise removal, contrast enhancement and image finalisation. These operations facilitate the accurate detection of ridges and valleys. Feature extraction then consists of identifying the minutiae present on the fingerprint. Each minutia is described by its position, orientation and type. All of this information constitutes the biometric template of the fingerprint, which will be used during the comparison phase.

3.1.4 Advantages and limitations of fingerprint recognition

Fingerprint recognition has several advantages, including high accuracy, relatively low sensor costs and ease of use. It is widely accepted by users and can be easily integrated into various automatic control systems. However, this technology also has certain limitations. Fingerprints can be altered by injuries, skin wear, or specific working conditions. In addition, there are risks associated with forgery or identity

theft, requiring the integration of liveness detection and data security mechanisms.

3.1.5 Comparison and decision-making

During use, the system compares the extracted template with those in the database by calculating a similarity score. Two modes are possible:

- **Verification (1:1)**: the system confirms the identity claimed by the user.
- **Identification (1: N)**: the system seeks to identify the user among all the stored templates.

The score obtained is then compared to a predefined threshold to decide whether access is granted or denied. The choice of threshold is a compromise between security and user-friendliness.

1. **Advantages and limitations**

Facial recognition offers several advantages: speed, minimal contact, remote identification and integration into video surveillance systems. It is particularly effective in environments with high foot traffic. However, it also has certain limitations. Performance can be reduced by variations in lighting, changes in expression, ageing, or accessories covering the face. In addition, the use of this technology raises ethical and legal concerns about privacy and surveillance, requiring a strict regulatory framework.

2. **Feature extraction**

The next step is to extract the distinctive features of the iris. Modern techniques use Gabor filters or Fourier transforms to robustly capture textural patterns. This information is converted into a **compact binary template** that uniquely represents the iris. This template is then stored in the database for future comparison. Its compactness and richness of information allow for fast and reliable identification, even in databases containing thousands of individuals.

3. **Comparison and decision**

During authentication, the template extracted from the iris presented is compared to those in the database using matching algorithms. A similarity score is calculated, and identity is validated if this score exceeds a predefined threshold. Two modes of operation are possible: **verification (1:1)**, to confirm a user's identity, and **identification (1: N)**, to find an individual among several templates. The decision threshold is chosen according to the level of security required, in order to limit false rejections and false acceptances.

4. **Advantages and limitations**

Iris recognition has many advantages:

- **High accuracy**: iris patterns are highly distinctive and stable over time.
- **Robustness**: little affected by age, illness or physical changes.
- **Security**: difficult to falsify or circumvent.

However, it also has some limitations. The technology requires specialised and expensive sensors, and performance can be affected by eye movement, excessive ambient light or certain eye disorders.

3.4 Voice recognition

Voice recognition is a biometric technique that identifies or authenticates an individual by analysing the unique characteristics of their voice. Each person has a distinct voice timbre, determined by the morphology of their vocal cords, the shape of their oral cavity, nose and pharynx, and their pronunciation habits. These parameters give the voice an individual acoustic signature that can be used for access control, secure telephony or surveillance systems.

Figure 14: Voice recognition

3.4.1 Acquisition and pre-processing

Voice acquisition is performed using microphones, which can be integrated into computers, telephones, or dedicated devices. The quality of the recording depends on the stance from the microphone, ambient noise, and speech clarity. Pre-processing aims to improve the signal and eliminate background noise, echoes, and interference. Techniques such as amplitude normalisation, bandpass filtering and noise

suppression are used to obtain a clear signal that can be used for voice feature extraction.

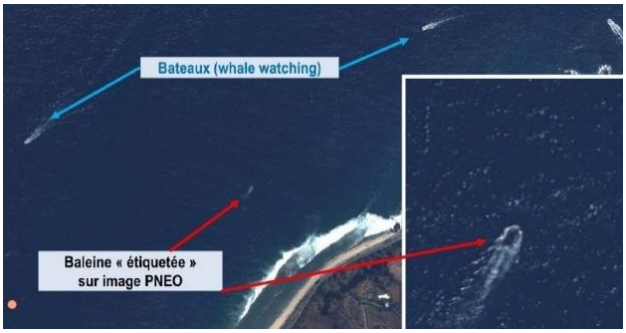


Figure 15: Voice acquisition is performed using microphones

3.4.2 Feature extraction

After pre-processing, the system extracts distinctive acoustic parameters, called **features**, which capture the unique aspects of the voice. These features may include the fundamental frequency, power spectrum, formants, and temporal modulation of the voice. Modern methods often use machine learning and neural network techniques to generate robust feature vectors that can compactly represent a user's voice identity. These vectors are stored as **voice templates** in a secure database.

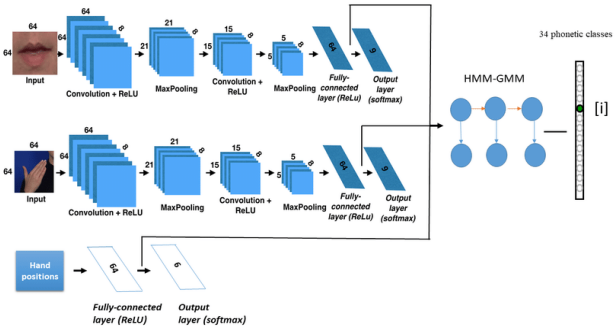


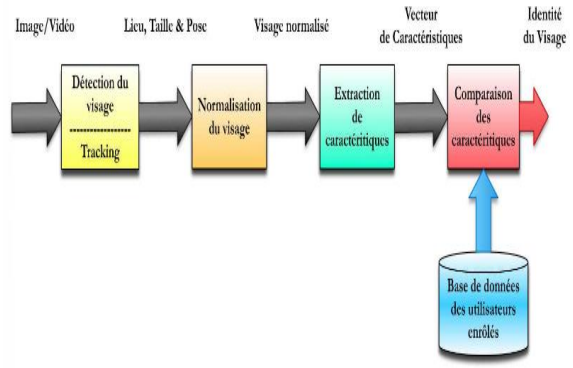
Figure 16: Voice templates

3.4.3 Comparison and decision

During authentication, the extracted voice template is compared to those stored in the database using voice recognition algorithms. A similarity score is calculated, and the identity is validated if this score exceeds a predefined threshold. Two modes of operation are possible:

- **Verification (1:1)**: confirms a user's identity.
- **Identification (1: N)**: identifies an individual among several templates.

The performance of the system depends on the choice of threshold, ambient noise and natural variations in the voice related to age, health or emotion.



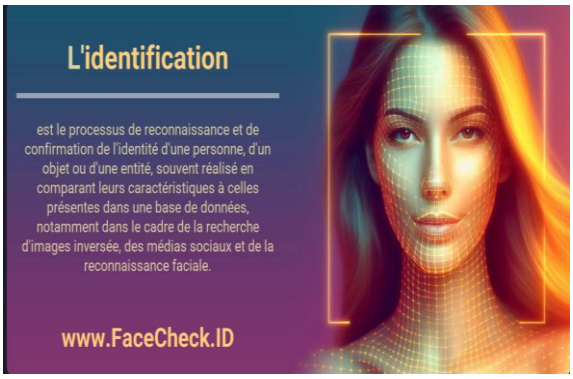


Figure 17: Comparison and decision authentication

3.4.4 Advantages and limitations

Voice recognition has several advantages: it is non-intrusive, does not require physical contact and can be used remotely. It is particularly suitable for telephone systems and environments where direct contact is limited. However, the voice can vary depending on emotion, fatigue, illness or environmental conditions, which can affect accuracy. In addition, it is more vulnerable to fraud attempts, such as imitation or recording, requiring the addition of liveness detection mechanisms or multimodal authentication.

4. Architecture of an automatic biometric control system

A biometric system comprises:

- A biometric sensor;
- A processing module;
- A biometric database;

- A decision module;
- A user interface.

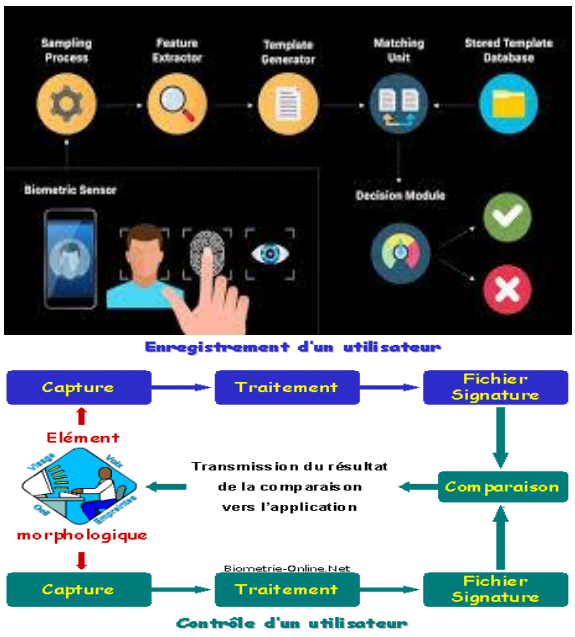


Figure 18: Architecture of an automatic biometric control system

An automatic biometric control system is designed to identify or authenticate an individual reliably and quickly, using their biological or behavioural characteristics. The architecture of these systems is based on several interdependent components that ensure the acquisition, processing, storage and comparison of biometric data.

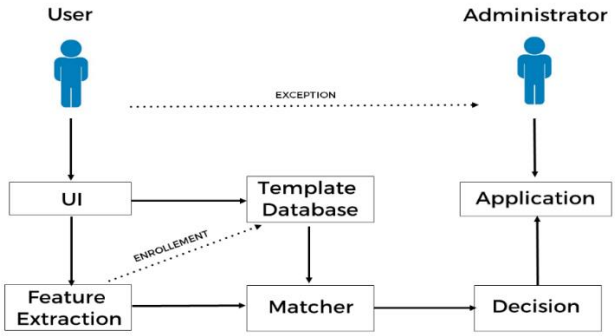


Figure 19: How the biometric system works

4.1. Acquisition of biometric data

Acquisition is the first step in the system. It relies on sensors adapted to the type of biometrics used: optical sensors for fingerprints, cameras for facial recognition, or infrared for iris recognition. This step collects the raw information needed for processing, ensuring the quality and accuracy of the data.

Figure 20: Acquisition of biometric data

4.2. Pre-processing and standardisation

The raw data collected undergoes pre-processing to improve its quality and make it usable. This stage includes noise reduction, standardisation of dimensions and orientation, and extraction of areas of interest. For example, for facial recognition, pre-processing aligns the face and corrects for lighting variations, while for fingerprints, it accentuates ridges and minutiae.

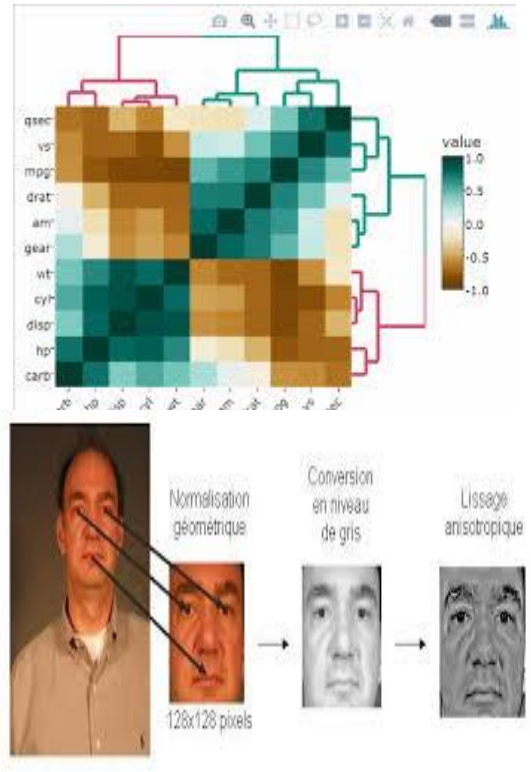


Figure 21: Pre-processing and standardisation

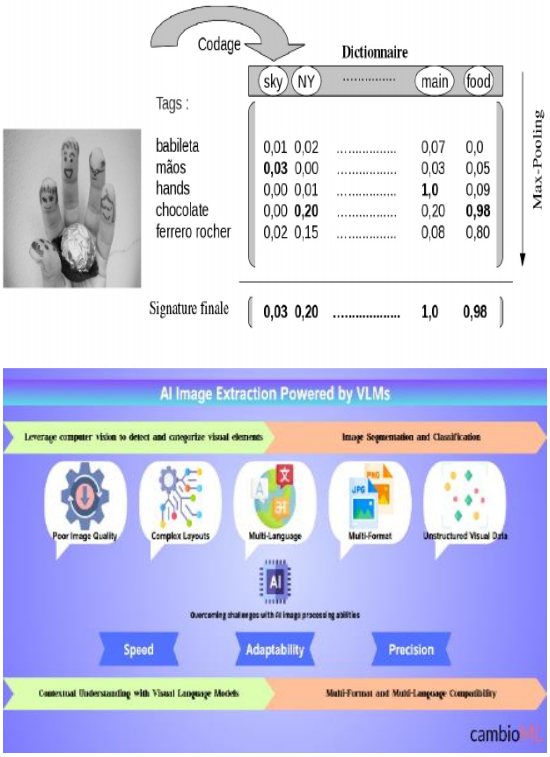


Figure 22: Extraction and encoding

4.3. Feature extraction and encoding

Feature extraction transforms pre-processed biometric data into a **digital template** representing the individual's unique information. This template is then encoded in a compact manner to facilitate storage and comparison. The effectiveness of this step directly determines the accuracy of the system, as the template must be sufficiently discriminating to distinguish between different individuals.

4.4. Biometric database

The extracted templates are stored in a secure database, which forms the core of the system. Data security is essential, as biometric information is sensitive and cannot be modified. Encryption, restricted access and intrusion protection mechanisms ensure the confidentiality and integrity of the templates.

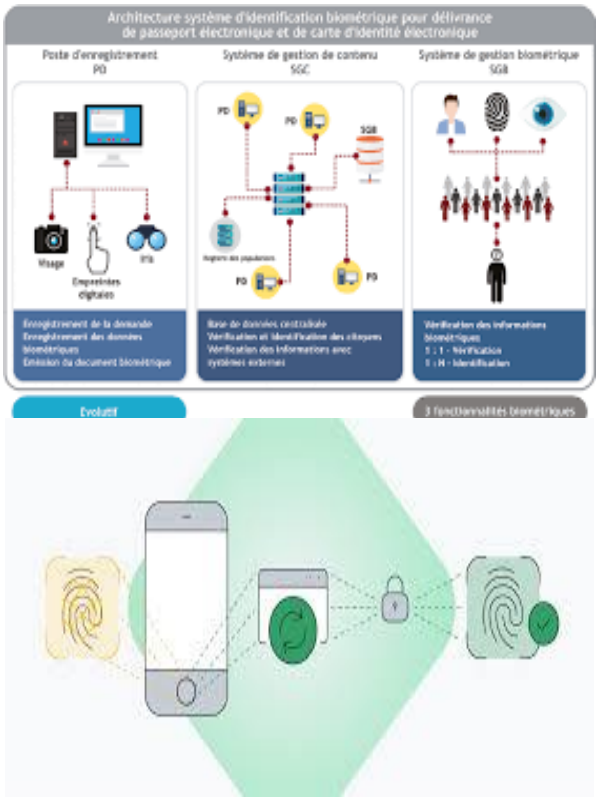


Figure 23: Biometric database

4.5 Matching and decision module

When a user attempts to authenticate, the system compares the extracted template with those in the database using matching algorithms. A similarity score is calculated and compared to a predefined threshold. Depending on the mode of operation (1:1 verification or 1: N identification), the system makes a decision to accept or reject.

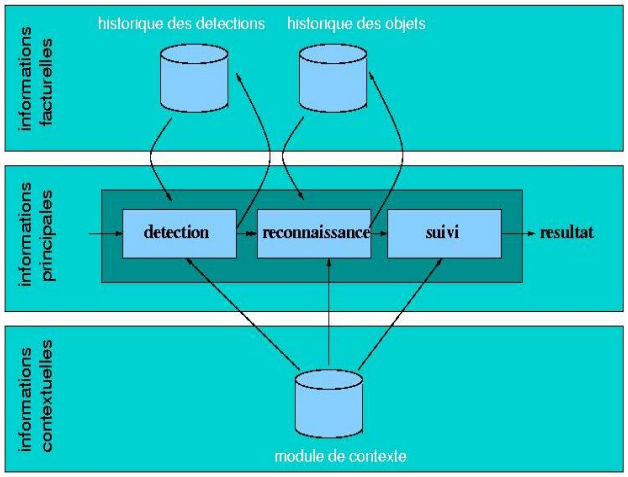


Figure 24: Matching and decision module

5. System implementation methodology

5.1 Needs analysis

Our choice of Mazenod University (UDMAZ) as an entity is located at 3145 Kasa-vubu Avenue in the NGANDA (Jamaica) district of the Kitambo commune, city-province of Kinshasa in the Democratic Republic of Congo.

In addition to the operating licence granted by Ministerial Decree No. 042/2008/MINESURS/CABMIN of 7 July 2008 and the admission to accreditation by Ministerial Decree No. 078/MINESU/CABIN.ESU/MML/KOB/2010 of 27 April 2010, recognised it as a "public utility institution" under the name Institut Supérieur Saint Eugene de Mazenod, this academic institution has benefited from two other Ministerial Decrees. As a "public utility institution" under the name Institut Supérieur Saint Eugene de Mazenod, this academic institution has benefited from two other Ministerial Decrees.

5.2 Choice of biometric technology

5.2.1 Presentation of the Mazenod University network model for academic fee access control

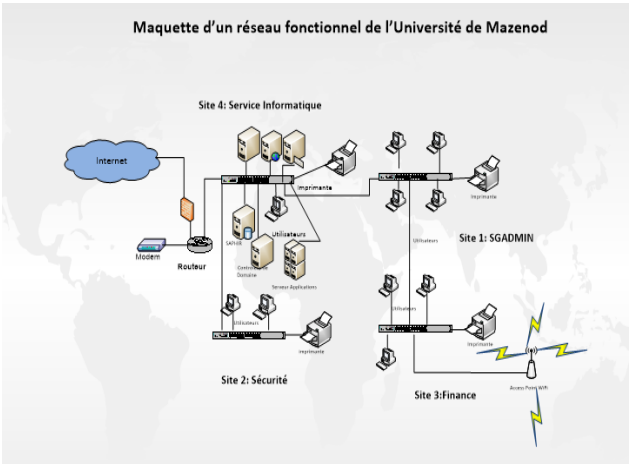


Figure 25: Model of a functional network for Mazenod University

5.2.2 Study of the technical solution

The study of the technical solution consists of precisely identifying the IT resources that will enable us to implement our IT system. We address two aspects, namely:

- Hardware resources;
- Software resources.

5.2.3 Hardware resources

The hardware on which our application will be developed is:

- ✓ **A server computer with the following specifications**
  - Intel Pentium M processor, 1 GHz speed;
  - 500 GB Seagate SATA hard drive (HDD);
  - 5 GB DIMM RAM memory;
  - 17-inch LCD screen;
  - 108-key AZERTY keyboard;
  - Optical mouse.

5.2.4 Software resources

Here is the software we will use to implement our application:

- ✓ Windows operating system (2008 server, Windows 10);
- ✓ Programming language: (C sharp);
- ✓ DBMS: MySQL;
- ✓ Enterprise Architect: Software for modelling with UML
- ✓ Microsoft Office 2016;
- ✓ Antivirus: Kaspersky or Norton and Symantec server.

5.3 System design

5.3.1 Non-functional requirements

Non-functional requirements are environmental and implementation constraints such as performance management, technical platform dependency, maintainability, scalability and reliability. The non-functional requirements of our system may be:

1. The system must be able to certify data security by authenticating each user who wants to access the system.
2. Access is possible by entering a username and password.
3. The system must guarantee data integrity and consistency.
4. The system must be interactive, reliable and easy to administer. The system must be easy to administer, capable of operating without errors, and display the processes carried out by the user.
5. The system must have a simple and user-friendly interface.
6. The system must report errors and avoid conflicts.

5.3.2 Technical choices

The development of this application allowed us to choose a standard UML modelling language and MySQL relational database management system, with C Sharp as the development environment and programming language.

5.3.3 Dynamic context diagram

In line with our UP approach, we recommend first establishing a context diagram to situate the domain of study in relation to other business processes.

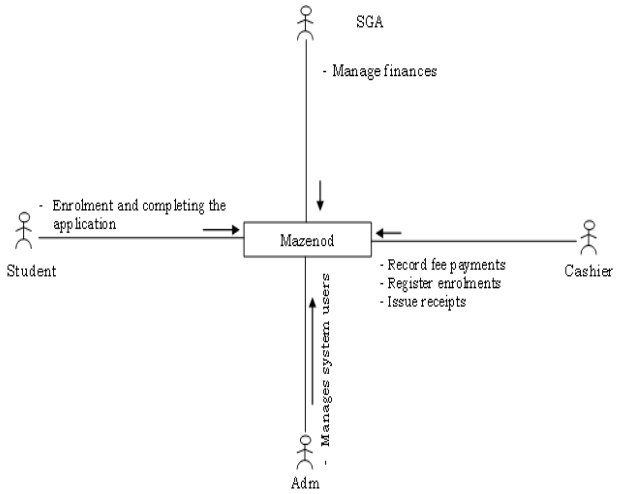


Figure 26: Dynamic context diagram

5.3.4 Developing use case diagrams

Based on the first use case developed in the "functional requirements" section, it is now possible to refine the analysis of the different cases. This analysis leads to the addition of several use cases, such as:

- ✓ **Authentication**: as our application will run on a web environment, it is important for us to introduce user authentication, as not everyone will have access to all the application's features.

Illustration of use cases with Enterprise Architect software

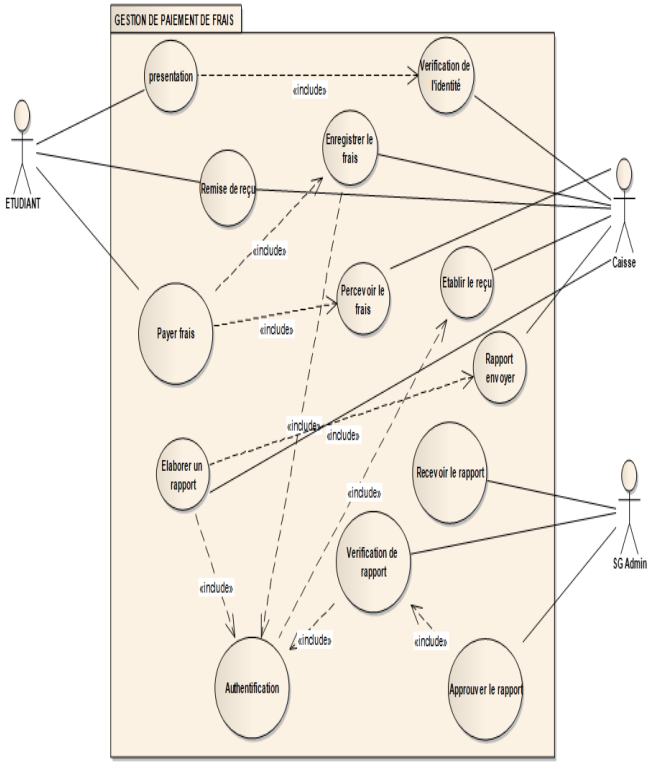


Figure 25: Use case diagram

5.3.5 Activity diagram

The activity diagram is one of the dynamic diagrams in UML; it is basically similar to a flowchart, showing the flow of actions in action. The basic elements of the activity diagram are as follows:

- Actions,
- Control flows between actions,
- Conditional branches (decisions),
- A start and one or more possible endings.

The activity diagram has a number of similarities with the state transition diagram, as it concerns the internal behaviour of operations or use cases. However, the behaviour referred to here applies to control flows and data flows specific to a set of activities and no longer to a single class. All you need to do is draw the different paths in the activity diagram that pass through all the transitions between actions. The concepts that are common or very similar between the activity diagram and the state transition diagram are:

- transition, ⟶
- initial node (initial state),
- final node (final state),
- ⊗ end node flow (output state),
- ◊ decision node (choice).
- The formalism remains the same for these control nodes.

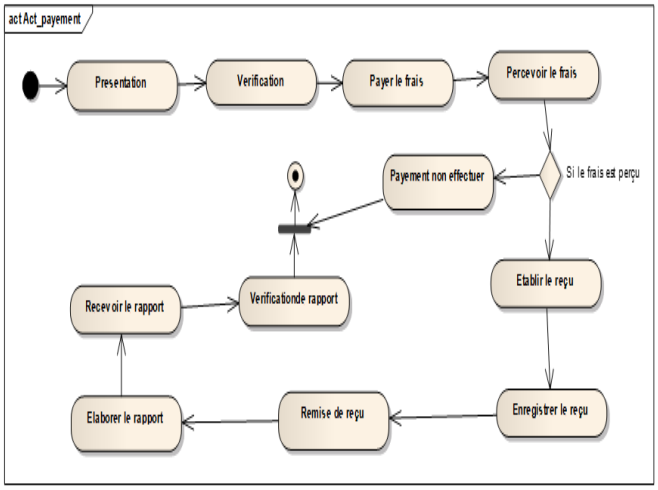


Figure 26: Activity diagram

5.3.6 Sequence diagram

Since a sequence is a flow of events occurring over time, its diagram allows us to give much greater expressive power to the various messages exchanged between the user and the system compared to the use case. The purpose of the sequence diagram is to represent the interactions between objects by indicating the chronology of exchanges.

5.3.7 Some concepts

A lifeline: represents all the operations performed by an object. A message received by an object triggers the execution of an operation. Feedback can be implicit (general case) or explicit using a return message. In this section on **sequence diagrams**, we will present the interactions of the system objects using a sequence diagram for each use case scenario.

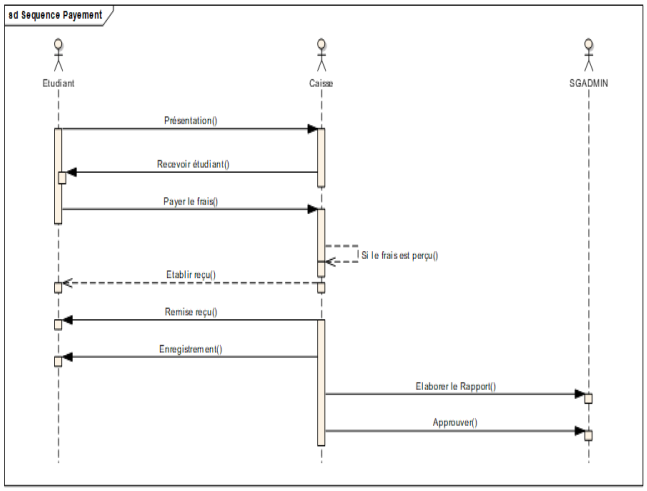


Figure 27: Sequence diagram for the "manage payment" use case

Sequence diagram for the "Authentication" use case:

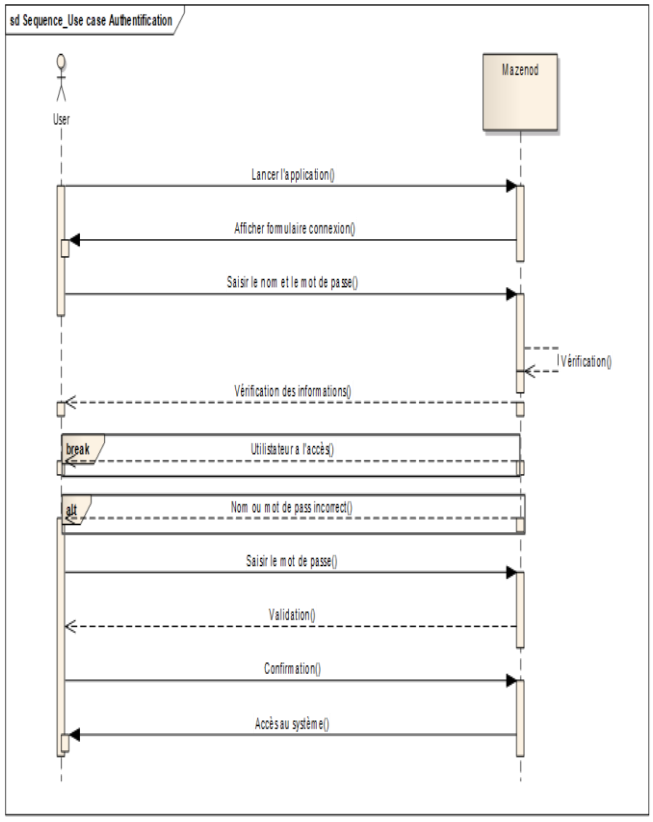


Figure 28: Sequence diagram for the "authentication" use case

5.4 Business class diagram

5.4.1 Definition and purpose

The class diagram is the focal point of object-oriented development. In analysis, its purpose is to describe the structure of the entities manipulated by users. In design, the class diagram represents the structure of object-oriented code or, at a more detailed level, the modules of the development language[1] .

Object-oriented design mainly requires a structural, static description of the system to be implemented in the form of a set of software classes, possibly grouped into packages. The best candidate classes are those resulting from an analysis of the domain (often also referred to as the business domain), i.e. the concepts manipulated by experts in the domain. The business class diagram Define the business concepts of the domain in the form of classes based on the identified actors and business processes of the system under study (control flow, data flow).

5.4.2 Class presentation for academic fee payment management

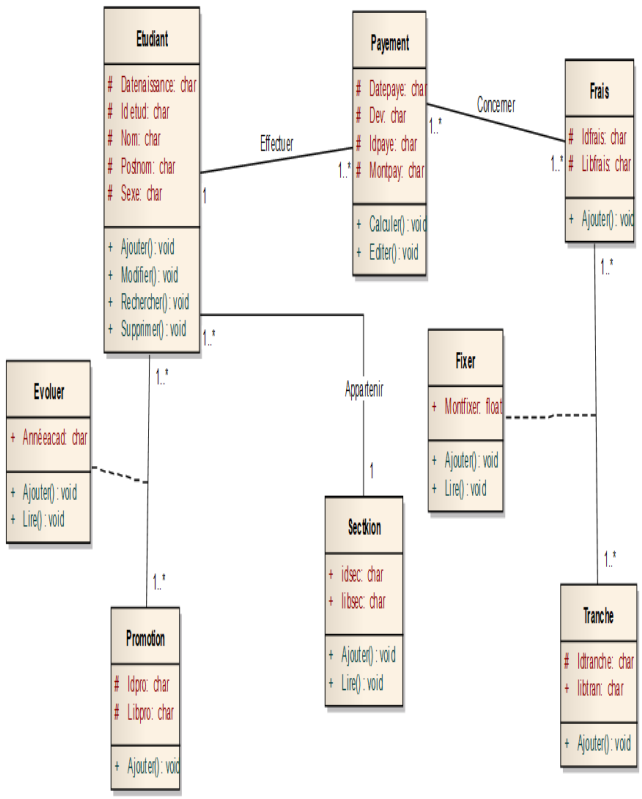


Figure 29: Class diagram

5.5 Implementation

5.5.1 Definition

Programming is the set of techniques and methods used to develop and codify a series of operations into an executable programme on a machine. A programme is a coordinated series of instructions recorded on a medium that allows a series of specific operations to be executed, as requested by a computer or automatic device.

5.5.1 Choice of programming language

A programming language is a computer language that allows a human being to write source code that will be analysed by a machine, usually a computer. With this in mind, we have made the judicious choice of the Visual Basic programming language. C# is used in the Windows platform to program applications and pass commands between applications; it is a subset of Windows, and this script is used only in certain specialised applications.[2] We have chosen C sharp in Visual Studio.

[1] Pascal R, **Les cahiers du programmeur UML2 Modélisé une application web** (UML2 Modelled Web Application), published by Eyrolles, 4th edition

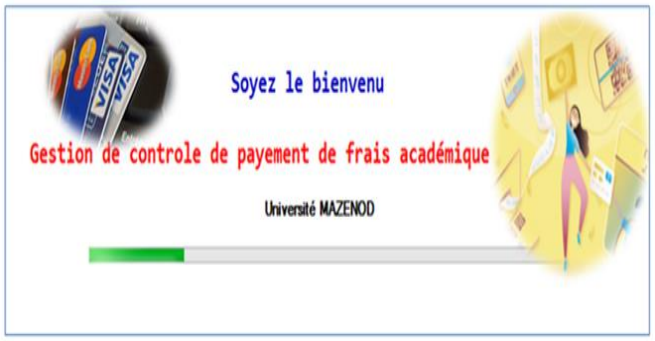
[2] MUSONGO R, Unpublished C# Course, G3INFO, UDMAZ, L2Infoi, 2022-2023

5.5.2 Presentation of interfaces and codes

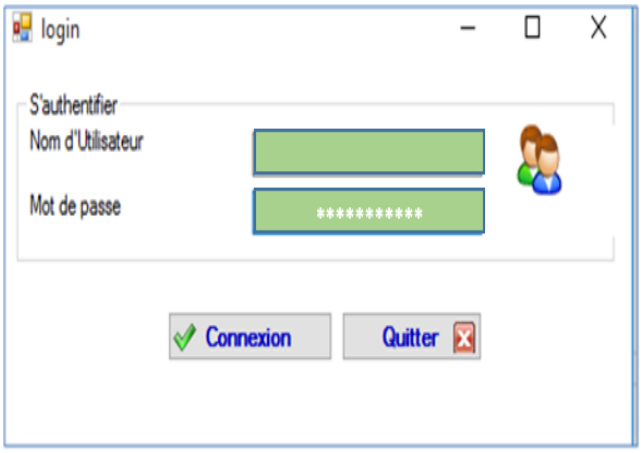
The previous chapter provided a brief overview of the different stages that led us to the creation of the database. This chapter is devoted to presenting some of the interfaces and codes of our software.

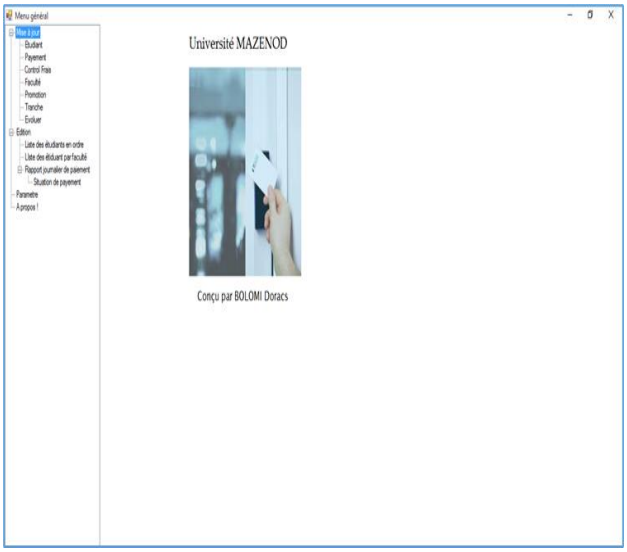
1. **Presentation of interfaces**

Login form:



General Menu Form:





Conclusion

The implementation of a biometric system for automatic fee control at Mazenod University represents a major advance in the field of security and access management. In this article, we have explored both the theoretical foundations and practical aspects of biometrics, highlighting its key role in the reliable identification and authentication of individuals. The various biometric techniques studied – whether physiological, such as fingerprint, facial or iris recognition, or behavioural, such as voice, signature and keystroke recognition – show that each method has its own specific characteristics, advantages and limitations.

Physiological techniques offer a high degree of reliability and stability. Fingerprint recognition, due to its uniqueness and technological maturity, remains one of the most widely used solutions. Facial recognition, on the other hand, combines ease of use and the absence of physical contact, but remains sensitive to variations in lighting, angle and expression. Iris and retina recognition are distinguished by their exceptional accuracy and resistance to fraud, although they require specific and costly sensors.

Behavioural techniques, such as voice recognition, signature recognition and keystroke recognition, offer complementary solutions that are particularly suited to remote applications or interactive systems. Although less stable than physiological characteristics, they add an extra layer of security, especially when combined with other biometric methods in **multimodal** systems. A study of the architecture of an automatic biometric control system has shown that its performance depends on the consistency and quality of its components: acquisition, pre-processing, feature extraction, secure storage and comparison module. Overall effectiveness depends on the seamless integration of these modules, as well as the optimisation of matching algorithms. A good system must not only provide fast and accurate identification, but also guarantee the protection of biometric data, which is sensitive and irreversible.

The adoption of biometric systems has the advantage of automatic control, which offers many benefits. It increases security, reduces fraud and identity theft, and facilitates the management of people flows. It also saves time and automates control processes, which is particularly useful in high-traffic areas such as airports, government offices and businesses. However, these systems are not without their limitations. Environmental factors, physiological and behavioural variations, and the risk of attacks or circumvention are major challenges. In addition, ethical and legal issues related to the collection and storage of biometric data require strict

regulatory oversight to protect individuals' privacy and prevent abuse.

Bibliographical references

[1] Ahmed, N., & Zafar, S. (2025). *Ethical and legal considerations in biometric data usage*. Journal of Ethics in Digital Technology.

[2] Agarwal, A., Ramachandra, R., Venkatesh, S., et al. (2024). *Biometrics in extended reality: a review*. Discover Artificial Intelligence. Springer Nature Link

[3] Aslam, M. S., & Aslam, S. (2025). *Touchless Biometrics: Securing a Post-Pandemic World*. Journal of Artificial Intelligence in Bioinformatics. ICCK

[4] Babnik, Ž., Peer, P., & Štruc, V. (2024). *eDifFIQA: Efficient face image quality assessment*. IEEE T-BIOM Articles – 2024 Q4. IEEE Biometrics Council

[5] Banerjee, S., Mittal, G., Joshi, A., et al. (2024). *Identity-aware facial age editing using latent diffusion*. IEEE T-BIOM Articles – 2024 Q4. IEEE Biometrics Council

[6] *Comprehensive survey: Biometric user authentication application, evaluation, and discussion* (2024). Computers and Electrical Engineering. ScienceDirect

[7] Hernandez, M., & Torres, J. (2024). *Behavioural biometrics: A continuous authentication approach*. IEEE Access.

[8] Gizachew Yirga T., Gizachew Yirga H., & Addisu E. G. (2025). *Cryptographic key generation using deep learning with biometric face and finger vein data*. Frontiers in Artificial Intelligence. Frontiers

[9] Gimba, U. A., Ariffin, N. A. B. M., Udzir, N. I., et al. (2025). *Enhancing biometric authentication through multimodal approach combining face and fingerprint recognition using CNN*. Discover Computing. Springer Nature Link

[10] Guo, J., Mu, H., Liu, X., et al. (2024). *Federated learning for biometric recognition: a survey*. Artificial Intelligence Review. Springer Nature Link

[11] Gupta, S., & Patel, D. (2024). *Palm vein recognition using deep neural networks*. Journal of Visual Communication and Image Representation.

[12] R. Sridevi & P. Shobana (2024). *Multimodal Security of Iris and Fingerprint with Bloom Filters*. arXiv preprint. arXiv

[13] Wang, Y., Gui, J., Shi, X., et al. (2025). *ColorVein: Colourful Cancelable Vein Biometrics*. arXiv preprint. arXiv

[14] *Emerging trends in biomedical trait-based human identification: A bibliometric analysis* (2024). SLAS Technology. ScienceDirect

[15] IEEE Biometrics Council (2025). *Biometrics on the rise*. IEEE Biometrics Council News. IEEE Biometrics Council

[16] Ren, X., Yang, S., Hou, S., et al. (2025). *Unsupervised gait recognition with selective fusion*. IEEE T-BIOM Articles – 2025 Q4. IEEE Biometrics Council

[17] Priya, K., Adak, C., Anand, S., & Chattopadhyay, S. (2025). *Offline signature verification: Exploring intra-variability across time intervals*. IEEE T-BIOM Articles – 2025 Q4. IEEE Biometrics Council

[18] Sadiku, M. N. O., Adekunte, P. A., & Sadiku, J. O. (2025). *Biometrics in Finance*. International Journal of Trend in Scientific Research and Development. IJTSRD

[19] ISO/IEC 30107 (2024). *Biometric presentation attack detection*. International Organisation for Standardisation.

[20] ISO/IEC 19794 (2024). *Information technology — Biometric data interchange formats*. International Organisation for Standardisation.

[21] Zhang, D., & Jain, A. K. (2024). *Advanced Biometrics: Techniques and Applications*. Journal of Biometrics and Authentication.

[22] Smith, J., & Lee, K. (2025). *Deep learning in multimodal biometric fusion*. Journal of Machine Learning Research.

[23] Chen, L., & Gupta, R. (2024). *AI-based spoof detection in face recognition systems*. IEEE Transactions on Information Forensics and Security.

[24] Kumar, V., & Singh, A. (2025). *Voice biometric authentication under noisy conditions*. International Journal of Speech Technology.

[25] Oliveira, P., & Rodrigues, R. (2025). *Keystroke dynamics in cybersecurity: A review*. Computers & Security.

[26] Martinez, A., & Choi, J. (2024). *Biometric sensors for wearable health monitoring*. Sensors Journal.

[27] Li, X., & Wang, Y. (2025). *Iris recognition efficiency in heterogeneous environments*. Pattern Recognition Letters.

[28] Park, H., & Kim, S. (2025). *Edge computing for privacy-preserving biometrics*. IEEE Internet of Things Journal.

[29] Nguyen, T., & Tran, L. (2025). *Smart card and biometric integration for secure authentication*. Journal of Security and Cryptography.

[30] Silva, R., & Costa, M. (2024). *Biometrics in IoT: Challenges and opportunities*. IEEE Communications Surveys & Tutorials.