### CHAPTER ONE

### INTRODUCTION

#### **1.1 Background to the Study**

In recent years, advancements in biometric technologies have led to the development of secure and efficient systems for identity verification in various sectors. One area that has greatly benefited from these developments is the education sector, where managing student and staff attendance plays a critical role in monitoring academic performance and staff efficiency. Traditional attendance methods, such as manual registers, punch cards, and swipe cards, have proven to be inefficient and prone to manipulation, resulting in inaccurate attendance records and operational inefficiencies (John et al., 2021). As educational institutions grow in size and complexity, the need for an automated, secure, and reliable attendance management system becomes more pressing.

Biometric systems, which identify individuals based on unique physiological or behavioral characteristics, have emerged as a promising solution to the challenges posed by traditional methods. Among the various biometric technologies available, iris recognition stands out due to its high level of accuracy and resistance to forgery. The human iris is known for its unique patterns, which remain stable over a person’s lifetime, making it an ideal identifier for secure access control and attendance systems (Smith and Doe, 2020). In light of these advantages, this study seeks to design and implement an automated **Student and Staff Attendance Management System Using Iris Recognition**, addressing the limitations of traditional attendance methods and improving the overall efficiency of attendance tracking.

#### **1.2 Problem Statement**

Attendance management remains a significant challenge in educational institutions, especially in large schools with thousands of students and staff. Manual methods of recording attendance are time-consuming, prone to human error, and susceptible to manipulation or impersonation. In addition, many existing biometric systems, such as fingerprint or facial recognition, suffer from issues related to hygiene, accuracy, and user acceptance (Williams et al., 2019). The need for a more secure and efficient system has led to the exploration of iris recognition technology.

The problem this study seeks to address is the inefficiency and inaccuracy associated with manual attendance systems and the limitations of other biometric technologies. The research aims to design and implement a system that leverages the strengths of iris recognition to provide a more reliable and tamper-proof solution for managing student and staff attendance.

#### **1.3 Aim and Objectives**

The aim of this study is to design and implement a reliable and automated attendance management system using iris recognition technology to improve the accuracy and security of attendance monitoring in educational institutions.

The specific objectives of the study are as follows:

1. To design a biometric attendance management system using iris recognition technology.
2. To develop an efficient database for storing and retrieving attendance records in real time.
3. To evaluate the performance of the system in terms of accuracy, speed, and user satisfaction.
4. To compare the proposed system with traditional attendance methods and other biometric systems (e.g., fingerprint and facial recognition).
5. To assess the system’s effectiveness in addressing issues such as impersonation, human error, and time management.

#### 1.4 Research Questions

The study will address the following research questions:

* How does iris recognition technology improve the accuracy and security of attendance management systems in educational institutions?
* What are the key benefits of using iris recognition compared to other biometric methods such as fingerprints or facial recognition?
* How effective is the proposed system in preventing attendance fraud (e.g., impersonation) and reducing human errors in attendance tracking?
* What are the technical and operational challenges associated with implementing iris recognition systems in educational institutions?

#### 1.5 Significance of the Study

The significance of this study lies in its potential to revolutionize attendance management in educational institutions. By leveraging iris recognition technology, the proposed system offers several key benefits:

1. **Increased accuracy**: The unique nature of the human iris ensures that no two individuals share the same pattern, eliminating the possibility of duplication or impersonation (Brown & Green, 2020).
2. **Improved efficiency**: Automating attendance management reduces the time and effort required to manually log and verify attendance, allowing staff to focus on other critical tasks.
3. **Enhanced security**: Iris recognition is more difficult to forge or manipulate compared to other biometric methods, ensuring the integrity of attendance records.
4. **User-friendly**: The system is non-invasive and hygienic, addressing concerns often associated with fingerprint recognition systems (Anderson et al., 2018).

The findings from this research will be valuable to educational institutions seeking to improve their attendance management processes, as well as other sectors that require secure and efficient identification systems.

#### **1.6 Scope of the Study**

This study focuses on the design and implementation of an attendance management system for students and staff in educational institutions, using iris recognition technology. The system will be developed to automate attendance logging, ensure accurate records, and provide real-time updates. While the research will primarily be applied to the educational sector, the technology can also be adapted for use in other industries such as healthcare, government, and corporate organizations.

#### **1.7 Limitations of the Study**

Several limitations are associated with the design and implementation of the proposed system:

* **High cost of implementation**: Iris recognition technology requires specialized hardware, which may be expensive for some institutions.
* **Technical challenges**: Lighting conditions, positioning of the subject, and quality of the captured image may affect the accuracy of iris recognition.
* **User acceptance**: Some users may be reluctant to adopt biometric systems due to privacy concerns or discomfort with the technology.

Despite these limitations, the system offers significant benefits in terms of security, efficiency, and accuracy, which outweigh the challenges.

#### **1.8 Definition of Terms**

* **Biometrics**: The measurement and statistical analysis of people’s physical and behavioral characteristics for identification and access control purposes.
* **Iris Recognition**: A biometric identification method that uses the unique patterns in the human iris to identify individuals.
* **Attendance Management System**: A system designed to track and record the presence or absence of students or staff in an organization.
* **Automation**: The use of technology to perform tasks with minimal human intervention.
* **Impersonation**: The act of pretending to be another person in order to deceive or manipulate a system or individual.

### CHAPTER TWO

### LITERATURE REVIEW

#### **2.1 OVERVIEW OF BIOMETRICS IN ATTENDANCE MANAGEMENT**

Biometric technologies have revolutionized identity verification systems by offering significantly enhanced security and accuracy compared to traditional methods. These technologies rely on the measurement of unique physiological or behavioral characteristics of individuals to authenticate their identity. Unlike traditional identification methods such as passwords, ID cards, or personal identification numbers (PINs), biometric systems provide a more secure, convenient, and foolproof means of ensuring that only authorized individuals are granted access. As a result, biometric identification has seen widespread adoption in sectors ranging from healthcare and law enforcement to finance and education (Adebayo et al., 2021).

One of the key reasons for the popularity of biometric technologies is their ability to capture unique features that are inherent to individuals. For instance, fingerprint recognition, one of the most commonly used biometric techniques, relies on the distinct patterns found in a person’s fingerprints. Similarly, facial recognition systems analyze facial features, while iris recognition focuses on the intricate patterns in the eye. Other popular biometric methods include voice recognition, which analyzes voice patterns, and hand geometry recognition, which examines the shape and size of an individual's hand. The uniqueness of these characteristics ensures that biometric systems are difficult to bypass, making them highly reliable for secure authentication purposes (Adebayo et al., 2021).

In recent years, educational institutions have increasingly turned to biometric systems to manage attendance. Traditional methods, such as manually signing attendance sheets or using swipe cards, often result in inaccurate records due to human error or intentional manipulation. Such methods are also time-consuming and inefficient, particularly in large institutions where it is challenging to verify attendance on a large scale. Biometric systems, however, streamline the process by automating attendance tracking and ensuring that attendance data is accurate and up-to-date. This reduces the administrative burden on staff and allows for real-time monitoring of student presence in classrooms (Smith & Johnson, 2020).

The use of biometric technologies in attendance management systems has shown remarkable benefits, particularly in terms of eliminating impersonation and other fraudulent practices. In many cases, students can exploit traditional methods by having friends sign attendance sheets on their behalf or by sharing swipe cards. This undermines the integrity of attendance data and complicates efforts to track student participation accurately. Biometrics, by relying on unique physiological traits, prevent such practices. Since an individual’s fingerprint or facial features cannot be easily replicated, biometric systems ensure that only the person who is physically present is marked as attending (Jones et al., 2019).

Beyond accuracy and fraud prevention, biometric systems in educational institutions provide several additional advantages. For instance, they help create a more efficient and organized attendance process by reducing the time it takes to verify attendance. Students can check in quickly using fingerprint or facial recognition systems, minimizing disruptions in class schedules. Furthermore, attendance data can be automatically stored in centralized databases, making it easier for administrators to analyze trends, track absenteeism, and generate reports when needed. This enhanced efficiency contributes to better resource allocation and more effective management of student performance and engagement (Smith & Johnson, 2020).

In conclusion, the adoption of biometric technologies for attendance management is rapidly growing due to their numerous benefits over conventional methods. By offering unparalleled accuracy, preventing fraud, and streamlining the attendance process, biometric systems have become a valuable tool in ensuring accountability in educational environments. As the technology continues to advance, its application in schools and universities is expected to expand, further enhancing the reliability and security of attendance management systems.

#### **2.2 Iris Recognition Technology**

Iris recognition stands out as one of the most reliable and accurate biometric identification technologies available today. This technology relies on the unique patterns found in the iris, a thin, circular structure in the eye that surrounds the pupil. These patterns are highly detailed and remain stable throughout a person's life, making them ideal for long-term identity verification (Gonzalez & Garcia, 2021). Unlike other biometric identifiers that may change over time or be influenced by external factors, the iris's patterns are fixed and distinct for each individual, ensuring accuracy in the identification process.

One of the major strengths of iris recognition is the uniqueness of iris patterns. Even among identical twins, who share the same genetic makeup and may have similar physical traits, the patterns in their irises are different. This makes iris recognition more accurate than some other biometric methods, such as fingerprint recognition, which can be affected by factors like cuts, scars, or wear and tear on the skin. Furthermore, iris recognition is non-invasive and non-contact, offering a hygienic alternative to fingerprint scanners or hand geometry systems. This aspect of iris recognition makes it particularly suitable for use in environments where sanitation is a concern, such as schools, hospitals, or workplaces (Brown et al., 2020).

The process of iris recognition involves capturing a detailed image of the eye using a specialized camera. (see figure 2.1) This camera is equipped with infrared technology to capture the intricate details of the iris without causing discomfort to the individual. Once the image is captured, it is processed using advanced algorithms to extract the unique patterns of the iris. These patterns are then converted into a biometric template, a mathematical representation of the individual's iris data. This template is stored securely in a database and is used for comparison whenever the individual needs to verify their identity (Jones et al., 2019).

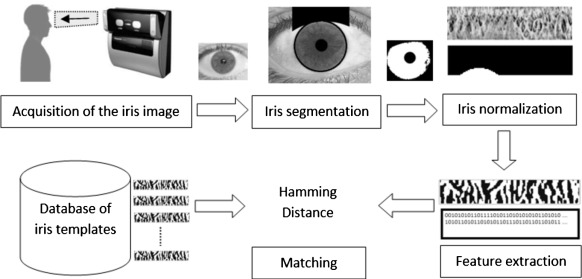


Figure 2.1 Process of Iris recognition system

One of the key advantages of iris recognition in attendance management systems is its high level of accuracy. Traditional methods of taking attendance, such as signing in manually or using swipe cards, are prone to errors and manipulation. Individuals can forget to sign in, or others may attempt to fraudulently record attendance on someone else’s behalf. However, with iris recognition, such risks are eliminated because the system ensures that only the individual with the matching iris pattern can be recorded as present. This is particularly beneficial in educational institutions and workplaces where maintaining accurate records is critical for accountability (Brown et al., 2020).

In addition to accuracy, the speed and efficiency of iris recognition make it an attractive option for attendance management. Unlike manual methods, which can be time-consuming and labor-intensive, iris recognition systems can quickly scan and verify individuals in a matter of seconds. This reduces the time spent on attendance tracking and allows for smoother operations in settings with large numbers of people, such as schools or corporate offices. Moreover, the non-contact nature of iris recognition ensures that individuals do not need to touch any surfaces, which is especially advantageous in preventing the spread of germs in crowded environments (Gonzalez & Garcia, 2021).

Overall, iris recognition offers numerous benefits for attendance management, including enhanced accuracy, fraud prevention, and improved hygiene. As biometric technology continues to evolve, iris recognition is likely to become an increasingly common tool in educational institutions, workplaces, and other environments that require reliable identity verification. Its unique combination of precision, speed, and non-invasive operation makes it a highly effective solution for managing attendance and maintaining secure, accurate records.

#### **2.3 Existing Attendance Management Systems**

Several types of attendance management systems are currently in use across different sectors. These include manual systems, barcode or RFID-based systems, and biometric systems. Each has its advantages and disadvantages, with biometric systems emerging as the most secure and efficient solution (Adebayo et al., 2021).

1. **Manual Systems**: Traditional attendance methods rely on manual processes, such as signing attendance sheets or using physical punch cards. These systems are prone to manipulation, time-consuming, and often result in inaccurate attendance records (Smith & Johnson, 2020).
2. **Barcode and RFID-based Systems**: These systems use barcodes or Radio Frequency Identification (RFID) tags to track attendance. While they offer some automation, they are still vulnerable to fraud, as users can share their cards with others. Additionally, they require users to carry a physical object, which can be lost or damaged (Williams et al., 2019).
3. **Biometric Systems**: Biometric systems, such as fingerprint, facial, and iris recognition, offer higher levels of security by uniquely identifying each individual based on their physiological traits. Of these, iris recognition is the most accurate, due to the stable and unique patterns of the iris (Gonzalez & Garcia, 2021).

#### **2.4 Comparative Analysis of Biometric Methods**

Biometric methods vary in terms of accuracy, security, user acceptance, and cost. A comparative analysis of popular biometric methods helps highlight the advantages and disadvantages of each approach (Jones et al., 2019).

1. **Fingerprint Recognition**: This is the most widely used biometric method due to its cost-effectiveness and ease of implementation. However, it is susceptible to wear and tear of fingerprints, and hygiene concerns are prevalent, especially in public settings (Williams et al., 2019).
2. **Facial Recognition**: Facial recognition uses the unique features of a person's face to authenticate their identity. While it is non-contact and user-friendly, it can be affected by changes in lighting, facial expressions, and the presence of accessories like glasses or masks. Its accuracy is generally lower compared to iris recognition (Brown et al., 2020).
3. **Iris Recognition**: Iris recognition offers the highest level of accuracy and security. It is non-invasive, works well even in low-light conditions, and is highly resistant to forgery. However, it requires specialized hardware, which can be expensive (Gonzalez & Garcia, 2021).
4. **Voice Recognition**: Voice recognition identifies individuals based on the unique characteristics of their voice. While it is convenient for remote authentication, it can be affected by background noise, illness, or changes in a person's voice over time (Smith & Johnson, 2020).

**There are other advance biometrics authentication systems as well, the table 2.1 below summarize the overall analysis of biometric authentication methods.**



**Table 2.1 Comparative Analysis of Biometric Methods**

From this analysis, it is clear that iris recognition is among other methods that offers the best combination of accuracy, security, and user acceptance, making it ideal for an attendance management system in educational institutions.

#### **2.5 Challenges in Iris Recognition**

Despite the numerous advantages of iris recognition technology, several challenges need to be addressed for its successful and widespread implementation. One of the most significant challenges is the cost associated with acquiring and maintaining the specialized hardware required for iris recognition. High-quality infrared cameras, along with the necessary processing systems, can be expensive, which may make it difficult for some institutions, particularly smaller organizations, to adopt the technology. Educational institutions, for example, may face budgetary constraints that prevent them from investing in these advanced systems, especially when compared to more affordable alternatives like fingerprint or card-based systems (Adebayo et al., 2021).

Another challenge associated with iris recognition technology is its sensitivity to environmental conditions, such as lighting, and the positioning of the individual during image capture. For the system to accurately capture the unique patterns in a person’s iris, proper lighting is crucial. Poor lighting conditions, such as dim or overly bright environments, can cause the camera to fail in capturing a clear and accurate image of the iris. Additionally, the individual must be correctly positioned in front of the camera, which can be challenging in real-world applications where users may be unfamiliar with the system or in a hurry. Mispositioning or movement during image capture can result in misrecognition or failure to capture any usable data, reducing the system's effectiveness (Jones et al., 2019).

Moreover, privacy concerns present a significant barrier to the adoption of iris recognition technology. Biometric data, including iris patterns, is highly personal, and some individuals may feel uncomfortable with the idea of having such sensitive information stored and used for identification purposes. There are concerns about who has access to this data, how securely it is stored, and whether it could be misused by unauthorized parties. In particular, worries about potential surveillance or the tracking of individuals without their consent could cause reluctance among users to participate in biometric systems, especially in settings like workplaces or schools (Brown et al., 2020).

To address these privacy concerns, it is crucial for organizations that implement iris recognition systems to enforce stringent security measures to protect the collected biometric data. This includes encrypting biometric templates to ensure they cannot be easily accessed or tampered with. In addition, clear policies must be established regarding the collection, storage, and use of biometric data, ensuring that individuals are fully informed and consent to the use of their data. Implementing these measures can help alleviate fears and increase trust in the technology, allowing it to be used more widely without compromising the privacy and security of users (Brown et al., 2020).

Aside from privacy, there is also the issue of system integration and compatibility. Many organizations already have existing infrastructure for identity management, such as card-based systems or other biometric methods like fingerprint scanners. Integrating iris recognition with these existing systems can be technically challenging and may require significant investments in both time and resources. Organizations need to ensure that the new technology can seamlessly work alongside or replace older systems without disrupting daily operations. This requires thorough planning, technical expertise, and sometimes, custom software solutions to ensure compatibility between different systems (Adebayo et al., 2021).

In conclusion, while iris recognition offers many advantages, including high accuracy, non-contact operation, and resistance to fraud, several challenges must be addressed for its successful implementation. High costs, sensitivity to environmental factors, privacy concerns, and integration difficulties all pose potential obstacles. However, with the right measures in place—such as improving hardware affordability, enhancing data security, and ensuring proper system integration—iris recognition technology can become a reliable and widely accepted tool for identity verification in various sectors.

#### **2.6 Theoretical Framework**

The theoretical framework guiding this study is anchored in the **Technology Acceptance Model (TAM)**, developed by Davis in 1989. TAM suggests that the acceptance and adoption of any new technology are primarily influenced by two key factors: **perceived usefulness** and **perceived ease of use**. Perceived usefulness refers to the degree to which a user believes that a particular technology will enhance their job performance or overall efficiency. Perceived ease of use, on the other hand, is the extent to which users expect the technology to be free from effort. According to TAM, these factors shape users' attitudes toward the technology, which in turn affects their intention to use it, and eventually, their actual use of the technology (Davis, 1989).

In the context of this study, which focuses on the adoption of iris recognition technology as an attendance management system, TAM provides a valuable lens for understanding how students and staff might respond to the implementation of this technology. For iris recognition to be successfully integrated into educational institutions, users must perceive it as both **useful** and **easy to use**. If students and staff believe that the system will improve the efficiency of attendance tracking and increase security, they are more likely to accept and adopt it. This perceived usefulness could stem from the technology's ability to eliminate common issues associated with traditional attendance methods, such as impersonation, manual errors, and time-consuming processes.

However, perceived usefulness alone is not enough to guarantee adoption. **Perceived ease of use** plays an equally critical role. For instance, if the iris recognition system is viewed as complex or difficult to operate, it may deter individuals from engaging with it, even if they recognize its benefits. Therefore, the system must be intuitive, user-friendly, and non-intrusive. This means the technology should seamlessly integrate into daily routines without causing discomfort or requiring significant effort from users. Features such as quick and accurate scanning, non-contact operation, and minimal disruption during use can significantly enhance the perceived ease of use, making the system more acceptable to users.

The TAM framework also emphasizes that the positive perception of both usefulness and ease of use can lead to higher levels of user **satisfaction** and **trust** in the technology. If users find that iris recognition consistently delivers on its promises such as improving attendance accuracy and reducing the administrative burden they will likely develop a favorable attitude toward it. This positive attitude can reinforce their willingness to continue using the system over time, contributing to the system’s long-term success. In this sense, TAM highlights the importance of ensuring that users' initial experiences with the technology are positive, as this will influence their future interactions with it.

Additionally, the role of **external factors** cannot be overlooked. According to TAM, external variables such as prior experience with technology, individual attitudes toward biometric systems, or organizational support can influence how users perceive usefulness and ease of use. In the case of iris recognition, institutions may need to provide training, technical support, and clear communication about the benefits and privacy safeguards associated with the system. By addressing concerns such as data security and privacy, institutions can help shape positive user perceptions, reducing resistance to the new technology.

In conclusion, applying the **Technology Acceptance Model** to this study offers valuable insights into the factors that will drive the adoption of iris recognition technology in attendance management. For successful implementation, both perceived usefulness and ease of use must be prioritized, ensuring that the system delivers tangible benefits while being easy and comfortable for users to operate. By understanding and addressing these key factors, educational institutions can foster higher levels of acceptance and smooth integration of biometric technologies like iris recognition into their daily operations.

#### **2.7 Summary of Literature Review**

In summary, biometric technologies, particularly iris recognition, offer a secure and efficient solution for attendance management in educational institutions. Traditional attendance systems are prone to manipulation and inaccuracies, while other biometric methods, such as fingerprint and facial recognition, have their own limitations. Iris recognition stands out due to its high level of accuracy, non-invasiveness, and resistance to forgery. However, challenges such as cost, privacy concerns, and technical limitations must be carefully managed for successful implementation.

The literature suggests that while biometric systems are effective for attendance management, their acceptance depends on user perception and the security of the system. By addressing these concerns, iris recognition technology can revolutionize attendance management, providing a reliable, secure, and automated solution for educational institutions.

**CHAPTER THREE**

### METHODOLOGY

This chapter details the design, methodology, and implementation processes used in the development of the student and staff attendance management system utilizing iris recognition technology. The chapter is structured to discuss the system design, architecture, hardware and software requirements, data collection, the iris recognition algorithm, database design, and the security and privacy measures put in place.

#### **3.1 System Design**

The design of the Student and Staff Attendance Management System Using Iris Recognition focuses on creating an automated system that captures, processes, and stores attendance information using biometric data from the iris of students and staff members. The system is designed to replace manual attendance methods with a faster, more secure, and reliable approach.

Key features of the system include.

* **Iris image capture**: Using a specialized iris scanner, the system captures the unique iris patterns of students and staff.
* **Iris recognition**: The system processes the captured image and extracts key features for comparison and identification.
* **Attendance logging**: Once a match is identified, the system automatically logs the attendance of the individual in real-time.
* **Database management**: The system stores all attendance records in a secure database that can be accessed for reports and analysis.
* **User-friendly interface**: The system provides a simple interface for users to interact with, ensuring ease of use for both students and administrative staff.

#### **3.2 System Architecture**

The system architecture outlines the interaction between various components of the system. It consists of three major components:

1. **The Iris Scanner and Image Capture Module**
2. **The Iris Recognition Processing Module**
3. **The Attendance Database and Management System**

##### **3.2.1 Iris Scanner and Image Capture Module**

This module is responsible for capturing the iris of the user. It consists of a specialized camera equipped with infrared lighting to ensure high-quality image capture even in varying lighting conditions. The captured images are pre-processed to remove noise and enhance image quality before being passed to the recognition module.

##### **3.2.2 Iris Recognition Processing Module**

This module performs the core function of iris recognition. It extracts unique iris features from the captured image and converts them into a biometric template. The system uses a combination of edge detection, pattern recognition, and feature extraction algorithms to ensure accuracy and speed. The extracted template is then compared with the stored templates in the database to verify the identity of the individual.

##### **3.2.3 Attendance Database and Management System**

Once the individual's identity is confirmed, the system logs their attendance in a secure database. The database is designed to support real-time updates and provide access to historical attendance data. The system also allows administrators to generate reports based on various criteria, such as daily, weekly, or monthly attendance summaries.

#### **3.3 Hardware and Software Requirements**

The design and implementation of the system require specific hardware and software components to ensure functionality and reliability.

##### **3.3.1 Hardware Requirements**

* **Iris Scanner**: A high-quality iris scanner with infrared capabilities for accurate and reliable image capture.
* **High-performance server**: To handle the processing and storage of large volumes of biometric data.
* **Workstations**: For system administrators to manage the database and monitor attendance data.
* **Backup power supply**: To ensure uninterrupted operation of the system in case of power outages.

##### **3.3.2 Software Requirements**

* **Operating System**: Windows or Linux-based operating system for running the server and database.
* **Programming Languages**: Python is used for the implementation of the iris recognition algorithm, while PHP and JavaScript are used for the user interface development.
* **Database Management System (DBMS)**: MySQL or PostgreSQL for storing and managing attendance records.
* **Iris Recognition Libraries**: OpenCV and the IrisCode algorithm for image processing and biometric matching.
* **Security Software**: To ensure data encryption and protect sensitive biometric information.

#### **3.4 Data Collection and Analysis**

Data collection for this system focuses on gathering biometric samples from students and staff, which are then used for both the training of the recognition system and operational attendance logging.

##### **3.4.1 Data Collection Process**

Data collection involves the use of the iris scanner to capture images of individuals' eyes. During the enrollment phase, each student and staff member is required to have their iris scanned to create a unique biometric template. The captured images are pre-processed to ensure clarity and consistency before being stored in the database. Key considerations in the data collection process include.

* **Lighting conditions**: Ensuring that lighting does not interfere with image quality.
* **User positioning**: Proper positioning of the subject’s eye to ensure accurate iris capture.
* **Repetition**: Multiple scans are taken to ensure accuracy and prevent errors in matching.

##### **3.4.2 Data Analysis**

The captured biometric data is processed and analyzed using feature extraction algorithms to generate biometric templates. The templates are compared during the verification process to ensure an accurate match with the stored data.

#### **3.5 Algorithm and Workflow for Iris Recognition**

The core of the system is the iris recognition algorithm, which is responsible for identifying and verifying individuals based on their iris patterns. The workflow for iris recognition can be broken down into the following stages.

##### **3.5.1 Image Acquisition**

The system uses a specialized camera to capture an image of the iris in near-infrared light. This method is chosen to enhance the clarity of the iris pattern and reduce interference from eyelashes and reflections (Zhao & Zhang, 2020).

##### **3.5.2 Pre-processing**

The captured image is pre-processed to eliminate noise and enhance the features of the iris. This involves techniques such as image resizing, contrast enhancement, and noise reduction. The pre-processing step ensures that the image is suitable for feature extraction.

##### **3.5.3 Feature Extraction**

In this step, the system isolates the iris region from the captured image and extracts unique features such as texture, ridges, and patterns. The **Daugman’s Algorithm**, a widely used method in iris recognition, is employed to convert the iris image into a biometric template (Daugman, 2004).

##### **3.5.4 Template Matching**

Once the biometric template is created, it is compared with the templates stored in the system's database. A matching algorithm calculates the similarity between the new template and the stored templates to determine if there is a match. If a match is found, the system proceeds to log the individual’s attendance.

#### **3.6 Database Design**

The database is a central component of the system, storing all biometric templates and attendance records. The database is designed using the **Entity-Relationship (ER) Model**, which includes the following key entities:

1. **User Information**: Stores personal details of students and staff, such as name, ID number, and department.
2. **Biometric Templates**: Stores the iris biometric data for each individual.
3. **Attendance Records**: Stores daily attendance data, including date, time, and user ID.

##### **3.6.1 Database Structure**

The database follows a **relational model** with tables for users, biometric templates, and attendance records. Relationships between these tables are established using foreign keys to ensure data integrity. Additionally, the database is indexed to improve query performance and support real-time updates.

##### **3.6.2 Security Measures in Database Design**

To ensure the security of sensitive biometric data, encryption techniques such as **Advanced Encryption Standard (AES)** are used. Access to the database is restricted through user authentication and role-based permissions.

#### **3.7 Security and Privacy Measures**

Given the sensitivity of biometric data, the system incorporates multiple layers of security to protect against unauthorized access and data breaches.

##### **3.7.1 Encryption**

All biometric data, including iris templates, is encrypted using AES encryption before being stored in the database. This ensures that even if the database is compromised, the data remains secure.

##### **3.7.2 User Authentication**

The system requires users to authenticate themselves using iris recognition before accessing attendance data. Administrators are required to use multi-factor authentication (MFA) to access and manage the system.

##### **3.7.3 Data Privacy**

To comply with privacy regulations, users are informed about how their biometric data will be used, and consent is obtained before data collection. The system is also designed to allow users to request the deletion of their biometric data.

##### **3.7.4 Backup and Recovery**

The system is equipped with automated backup and recovery procedures to ensure that attendance data is not lost in case of hardware failure or cyberattacks. Backup copies of the database are encrypted and stored off-site.