Project Semester 4 (IoT)

Socio-Technical Analysis Report

Project Title: RobotProject1: Micro:bit Robot with Face Recognition

Student Name: Xuanru Guo

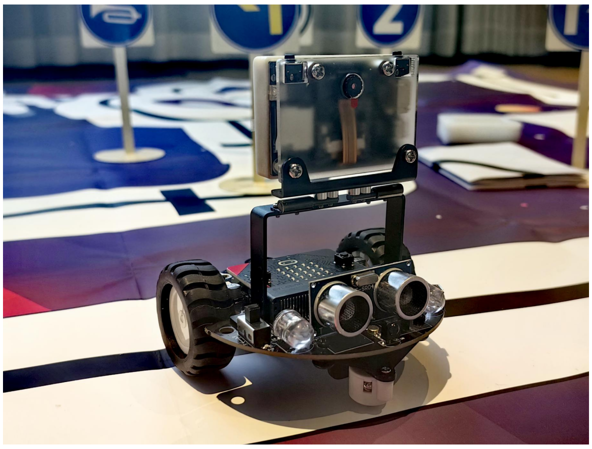
Student Id: 202283890028

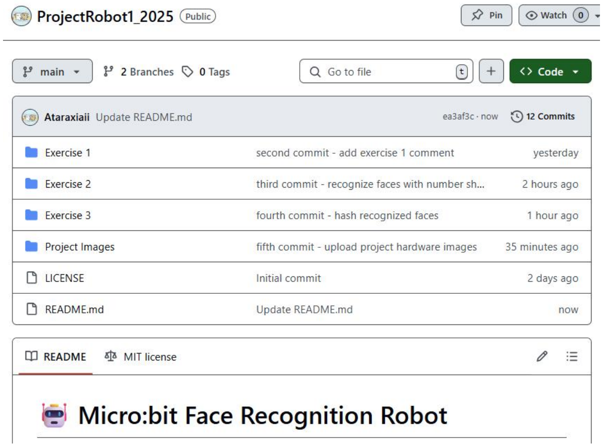
1. Project Outline and Objectives

RobotProject1 innovatively combines microcontroller programming (utilizing Micro:bit components and the K210 visual processor), Python scripting, and the application of the Scrum framework. It requires us to implement core functionalities, ranging from LED matrix displays to facial data encryption, while maintaining strict version control via GitHub.

As a hands-on Agile learning project, it bridges theoretical concepts with engineering implementation, ultimately delivering comprehensive outcomes including a functional robot prototype and demonstration video.

RobotProject1 helps students and developers gain interdisciplinary knowledge through real-world applications. This integrated approach enhances hands-on skills and deepens understanding of system integration and problem-solving. The project follows an Agile development model, emphasizing iterative progress and continuous feedback, allowing participants to grasp core Agile principles. Additionally, the implemented features, such as facial recognition and data encryption, are key technologies in smart devices and IoT. Building these functions firsthand provides a solid foundation for further development in these areas.





ProjectRobot1_2025 Public

2 Branches 0 Tags

Ataraxiaii Update README.md ea3af3c · now 12 Commits

Exercise 1	second commit - add exercise 1 comment	yesterday
Exercise 2	third commit - recognize faces with number sh...	2 hours ago
Exercise 3	fourth commit - hash recognized faces	1 hour ago
Project Images	fifth commit - upload project hardware images	35 minutes ago
LICENSE	Initial commit	2 days ago
README.md	Update README.md	now

Micro:bit Face Recognition Robot

2. Functional Requirements

RobotProject1 aims to develop a Micro:bit-based robot with three core functions, all implemented using Python within an Agile development framework:

a. **Display numbers on an LED matrix:** Control the LED matrix on the Micro:bit to show specific information or status.

b. **Recognize and match faces to specific numbers:** Utilize facial recognition technology to associate different faces with preset numbers, enabling personalized displays and interactive functionalities.

c. **Secure facial data through hashing:** Encrypt and store facial data securely by hashing it, ensuring user privacy.

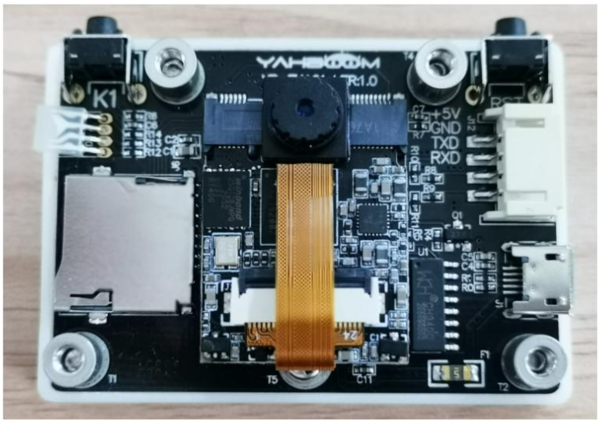
3. Technologies Used

The project utilizes a Micro:bit V2 development board as the core controller, communicates with a K210 vision module equipped with a dual-core RISC-V processor via the I2C interface, and employs a lithium battery power supply to provide stable 5V output for reliable system operation.

a. **Micro:bit V2 Development Board:** Serves as the central control unit in the face recognition system, leveraging its compact size and versatile I/O capabilities to connect various hardware components. It communicates with the K210 vision module through the I2C interface and drives a 5x5 LED matrix to display facial recognition results.

b. **K210 Vision Module:** Equipped with a dual-core RISC-V processor, it handles image data processing and performs facial recognition tasks.

c. **Lithium Battery Power Supply:** Provides stable output to ensure reliable operation of the vision processing unit and other peripheral components.



The project employs Python for control logic and algorithm implementation, uses Microsoft MakeCode for Micro:bit for rapid prototyping, leverages GitHub for code version management, and integrates a pre-trained YOLO model along with the hashing algorithm for facial recognition and data encryption.

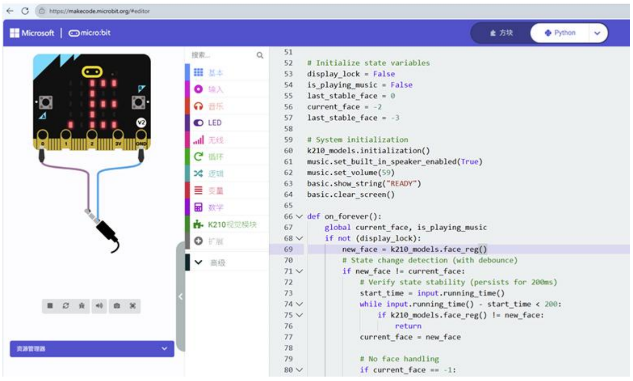
a. **Python Programming Language:** Used for writing control logic and implementing facial recognition algorithms, including development within Mu Editor.

b. **Microsoft MakeCode for Micro:bit:** Offers an intuitive programming environment for the Micro:bit that supports both block-based coding and Python, facilitating rapid prototyping.

c. **GitHub for Code Version Management:** Utilized for managing code and version control, ensuring security and traceability of the project's codebase.

d. **Trained YOLO Models:** Used to enhance the accuracy and efficiency of facial recognition.

e. **Hashing Algorithms**: Applied to securely store facial data by encrypting it, protecting user privacy.



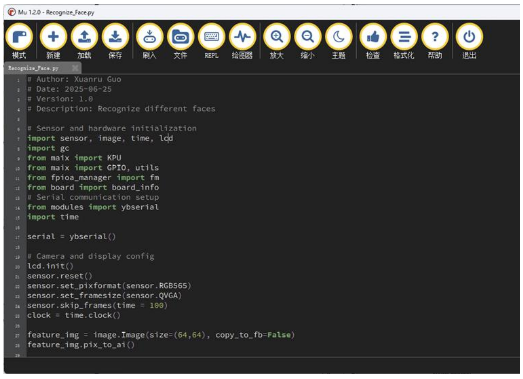
```python

# Initialize state variables
display_lock = False
is_playing_music = False
last_stable_face = 0
current_face = -2
last_stable_face = -3

# System initialization
k210_models.initialization()
music.set_built_in_speaker_enabled(True)
music.set_volume(59)
basic.show_string("READY")
basic.clear_screen()

def on_forever():
    global current_face, is_playing_music
    if not (display_lock):
        new_face = k210_models.face_reg()
        # State change detection (with debounce)
        if new_face != current_face:
            # Verify state stability (persists for 200ms)
            start_time = input.running_time()
            while input.running_time() - start_time < 200:
                if k210_models.face_reg() != new_face:
                    return
            current_face = new_face

            # No face handling
            if current_face == -1:
```



```python
# Author: Xuanru Guo
# Date: 2025-06-25
# Version: 1.0
# Description: Recognize different faces

# Sensor and hardware initialization
import sensor, image, time, lcd
import gc
from maix import KPU
from maix import GPIO, utils
from fpioa_manager import fm
from board import board_info
# Serial communication setup
from modules import ybserial
import time

serial = ybserial()

# Camera and display config
lcd.init()
sensor.reset()
sensor.set_pixformat(sensor.RGB565)
sensor.set_framesize(sensor.QVGA)
sensor.skip_frames(time = 100)
clock = time.clock()

feature_img = image.Image(size=(64,64), copy_to_fb=False)
feature_img.pix_to_ai()
```

4. Social Analysis and Issues

In this section, we will consider the broader social, human, legal and ethical issues pertaining to our project.

4.1. Privacy Issues

In the RobotProject1 project, privacy issues are of paramount importance. To comprehensively evaluate and address these potential privacy risks, we will use the ISD Privacy Framework to analyze four dimensions: physical, social, psychological, and informational.

Physical Dimension: The robot is a standalone device, allowing users to freely choose whether to use it in their own environment. This means that the robot does not invade users' private spaces. For example, users can choose to use the robot in a relatively isolated workspace or office, ensuring their physical solitude remains undisturbed. Additionally, the robot does not need to operate within the user's personal space unless they actively place and activate it.

Social Privacy: Users can turn off the robot at any time, stopping interaction with it. This ensures that users have full control over when they wish to engage or disengage from interactions. Moreover, users can choose whether to allow others to observe their interactions with the robot. By doing so, users maintain autonomy in social interactions and avoid unnecessary social pressure.

Psychological Privacy: The technology used by the robot is non-intrusive; it does not collect data without user consent and does not cause psychological harm through voice output or other means. All interactions are transparent and controllable, ensuring users always know what the robot is doing and why. For instance, when facial recognition fails, the LED display shows an "X" rather than emitting potentially distressing sounds or visual cues. This design helps protect users' mental health by avoiding negative emotions due to misunderstandings or accidental triggers.

Informational Privacy: All collected data is stored locally, and users can delete this data at any time. Furthermore, facial recognition data is encrypted using the algorithm, further safeguarding user privacy. Before starting to use the robot, users are required to fill out an informed consent form, detailing what data the robot will collect and how it will be used. This not only complies with legal requirements but also enhances users' trust in the system. Users can easily delete all personal information stored on their devices, thereby minimizing privacy risks as much as possible.

4.2. Data Protection Issues

In the RobotProject1 project, data protection is a core consideration during design and implementation. We refer to key principles of the General Data Protection Regulation (GDPR), including data minimization, data subject rights, transparency, and security safeguards, to ensure that user data is properly handled throughout its lifecycle.

a. Data Minimization

The robot only collects facial images of authorized users for identification purposes and does not record or store any unnecessary personal information. For example, it does not collect names, contact details, or other identifying information. All data collection serves specific functions such as displaying matching numbers or triggering music playback.

During use, the robot only collects the owner's facial data and does not automatically record other unnecessary information. This means that even if multiple people are in the same environment, the robot will not indiscriminately collect everyone's facial data unless they explicitly agree and are recognized as legitimate users by the system.

b. Data Subject Rights

Data owners have full control over their facial data. Users can delete all personal data stored on their device at any time through simple operations. Additionally, users have the right to access, correct, or request restrictions on the processing of their data.

Before starting to use the robot, users are required to fill out an informed consent form, detailing what data the robot will collect, how it will be used, and why it is needed. Users can choose whether to continue using the robot and have the right to revoke consent at any time.

c. Transparency

Organizations must clearly inform data subjects about the purpose and intended use of their data before collecting it. In the RobotProject1 project, all data collection activities are performed with the user's knowledge. For instance, when first starting up, the system prompts users to read and agree to the privacy policy, which explains the data usage and storage methods in detail.

The robot displays the current status to users during each recognition process, such as "Recognizing," "Recognition Successful," or "Recognition Failed." This transparency not only enhances user experience but also ensures that users always know what the robot is doing.

d. Security Safeguards

To prevent unauthorized access and processing, the project employs several technical measures. All collected facial data undergoes real-time feature hashing using the PBKDF2-HMAC-SHA256 algorithm with 50 iterations, converting raw biometric data into irreversible encrypted values stored locally. This method effectively prevents sensitive information leaks and ensures that even if data is stolen, it cannot be easily reversed.

The robot does not transmit collected data to external networks or third-party servers. All data is stored locally on the device, and only authorized users can access this data. This physical isolation mechanism further reduces the risk of data breaches.

4.3. Intellectual Property

In the RobotProject1 project, intellectual property (IP) considerations are crucial. We need to evaluate whether the software and hardware components we intend to use might infringe on others' IP rights, including copyright, patents, and other forms of intellectual property. Additionally, we must consider whether marketing or selling the project could potentially infringe on the IP rights of existing products in the market.

a. The Hardware and Software Used

The RobotProject1 project uses open-source development tools and programming languages such as Python, Microsoft MakeCode, and Mu Editor. These tools and languages typically adhere to open-source licenses that allow free use, modification, and distribution, provided the license terms are followed. Therefore, using these tools and languages does not infringe on any third-party IP rights.

The hardware components used in the project, including the Micro:bit V2 development board and K210 vision module, are manufactured based on publicly available technical specifications and standards. These hardware components are either open-source hardware or commercial products used under legitimate licensing. For example, the Micro:bit V2 development board is provided by the non-profit organization Micro:bit Educational Foundation, with its design documents and related resources openly accessible. The K210 vision module also adheres to relevant technical standards and licensing agreements, ensuring legal usage.

The code libraries and files used in the project, such as the YOLO model for facial recognition and the hashing algorithm, are released under open-source licenses. The use of these libraries not only complies with open-source community standards but also avoids the risk of infringing on others' IP rights. All external libraries used have been carefully reviewed to ensure they meet the requirements of their respective open-source licenses.

Custom code developed within the project has been independently written by team members without using any copyrighted third-party code snippets or proprietary technologies. This ensures that all custom code in the project is original and does not pose an infringement risk.

b. Potential IP Issues if Marketed/Sold

Before marketing the RobotProject1 project, a comprehensive market survey should be conducted to identify any similar functionalities or designs in existing products. Although the core features of the project (such as facial recognition and LED matrix display) may not be technologically unique, the specific implementation and user experience design should aim to avoid direct conflicts with existing products. To further mitigate the risk of IP infringement, it is advisable to conduct detailed patent searches and analyses before marketing the project.

4.4. Stakeholder and Risk Analysis

In the RobotProject1 project, it is essential to identify stakeholders — individuals or organizations who may be affected by the system and assess both positive and negative impacts. Furthermore, strategies should be developed to minimize risks and maximize benefits.

a. Stakeholders

The primary stakeholder in this project is the owner of the robot (i.e., the end user), as the device is designed for personal use without involving third-party data sharing or cloud connectivity.

b. Positive Impacts

The robot provides personalized feedback through facial recognition (displaying numbers or playing music), improving human-machine interaction.

As an embedded AI-based project using Micro:bit and K210 modules, it serves as a practical tool for students to learn about hardware, software, and privacy protection.

Users have full control over the system, including the ability to delete data or turn off the device at any time.

c. Negative Risks

- Physical Safety Risks: While the lithium battery used has low power consumption and built-in voltage regulation, there is still a slight risk of overheating or fire if the battery degrades or charging management fails. During installation, improper handling of tools (e.g., soldering iron, screwdrivers) may lead to finger cuts or burns.

- Privacy and Data Security Risks: Although data is stored locally and encrypted, if the robot is lost and accessed by unauthorized persons, sensitive information could potentially be extracted. Though rare, incorrect facial recognition might result in unintended responses (voice output), causing temporary discomfort.

- Technical Reliability Issues: Recognition Failure or Delayed Response: If the vision module's performance is inadequate or the algorithm is poorly optimized, it may lead to recognition errors or delayed reactions, affecting user experience.

d. Risk Mitigation Strategies

- Reducing Physical Risks: Use a standard lithium battery with overcharge and over-discharge protection circuits. Include clear safety instructions and assembly guidelines in the user manual to prevent accidental injuries. Recommend wearing protective gear (e.g., gloves, goggles) during assembly.

- Preventing Data Leakage: Encrypt all sensitive facial data using the PBKDF2-HMAC-SHA256 hashing algorithm, ensuring irreversibility. Provide a one-click data deletion function so users can erase all local data instantly. Avoid internet connectivity to eliminate the possibility of remote attacks or data transmission.

- Improving System Stability: Train and test the facial recognition model thoroughly to ensure high accuracy and low error rates. Optimize code logic to reduce lagging or system crashes. Offer clear user instructions to help users operate the robot correctly and safely.

5. Technical Analysis and Design

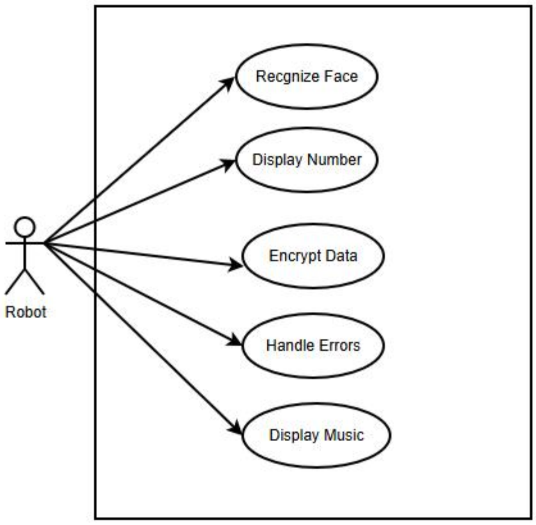
This section provides a comprehensive technical blueprint of the face recognition robot system, aligning hardware/software implementations with the social considerations outlined in Chapter 4. The design emphasizes ethical deployment through modular architecture and privacy-preserving data handling.

5.1. Functional Design and Non-Functional Requirements

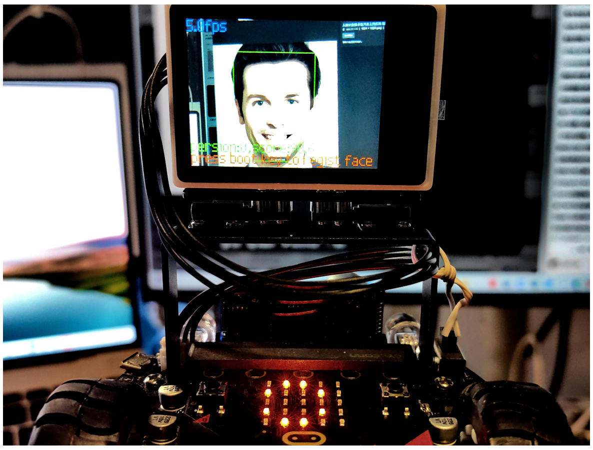
In this part, we will detail what the system will do and how it will do it. Use case diagrams and other UML diagrams may be helpful here. We will also discuss non-functional requirements to ensure that the social issues previously considered are addressed.

a. Functional Design

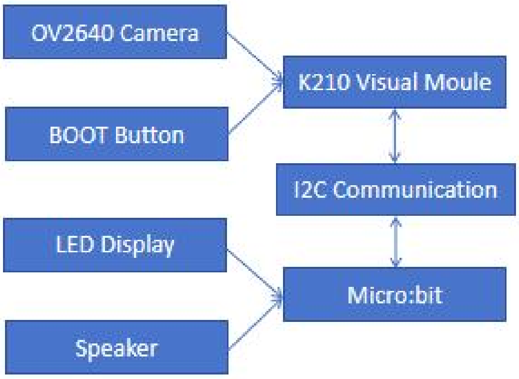
The design objective of the RobotProject1 project is to build a robot system with face recognition capabilities that can perform data collection, processing, and feedback locally, while ensuring the system's security, privacy, and usability.



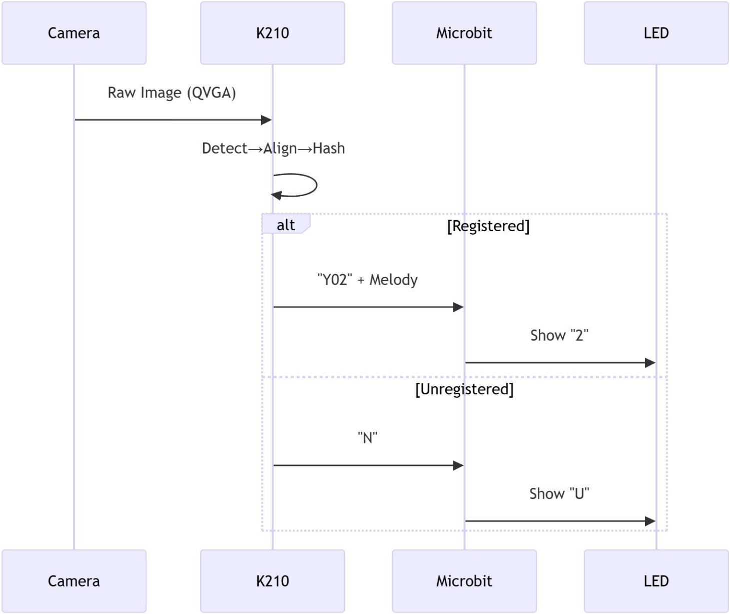
The core functionality of the system revolves around the acquisition, recognition, and response to facial images, combined with the Micro:bit platform’ s LED matrix for visual output. To achieve these functions, the development process spans multiple stages, from hardware assembly to software programming.



At the start of the project, we created a GitHub repository to manage code version control and team collaboration. This approach not only helps track every code modification but also ensures consistency and coordination when multiple developers are involved. Subsequently, the robot was assembled using the Micro:bit V2 development board and the K210 vision module. The Micro:bit serves as the main control unit, responsible for driving the LED matrix, receiving user input, and communicating with the K210 module, while the K210 handles image capture and face detection by running a pre-trained face recognition model.



At the software level, the system implements several key functionalities. First, an image display function utilizes the 5x5 LED matrix on the Micro:bit to show numbers or patterns, providing users with intuitive interactive feedback. Second, the face recognition module captures real-time images using the OV2640 camera attached to the K210 module, performing face detection and feature extraction. The system then associates the recognized face ID with a predefined number and displays the corresponding result on the LED screen. In addition, all extracted facial feature data is encrypted using a hashing algorithm to prevent raw biometric information from being directly accessed, thereby enhancing the system's data security.



b. Non-Functional Requirement

To ensure that the system not only meets functional expectations but also performs well in terms of user experience and social ethics, this project has established several non-functional requirements. Firstly, in terms of performance, the system must possess a certain level of real-time response capability, being able to process at least 30 frames per second, ensuring smooth and timely facial recognition.

Secondly, security is a critical consideration in the design, whereby all data concerning user privacy, especially facial feature information, should be handled with encrypted storage to prevent unauthorized access and potential data breaches.

Moreover, the system emphasizes usability in its design, ensuring that the operation interface is simple and intuitive so that even non-professional users can easily complete basic operations such as startup, interaction, and shutdown. For instance, users can trigger main functions through simple physical buttons.

Regarding privacy protection, the system strictly adheres to the principle of localized data processing, where all collected data is processed and stored solely on the device end, without uploading to any network servers or cloud platforms. Users have full control over their data and can delete stored information at any time. Additionally, before first use, the system will clearly inform users of the purpose of data collection and obtain their informed consent to ensure that the entire data processing flow complies with ethical standards and legal requirements.

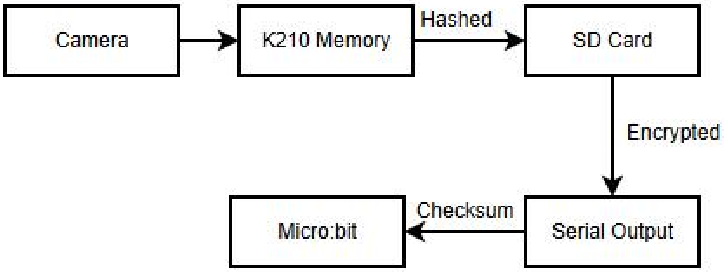
5.2. Data Requirements and Design

In this part, we will provide detailed information on data collection, storage methods, and representation formats, considering appropriate data protection measures.

At the data level, the design of the RobotProject1 project follows the principles of minimal data collection and local processing to comply with data protection regulations such as the GDPR. The system only collects necessary facial images with the user's explicit consent and performs all data processing and storage locally, without any form of remote transmission or cloud-based storage.

Data collection primarily relies on the OV2640 camera connected to the K210 module. This camera is capable of capturing low-resolution images that meet the basic requirements for face recognition. After image data is captured, it undergoes preprocessing on the K210 chip, where key facial feature vectors are extracted. These feature vectors are then used to compare against pre-registered facial templates for identity verification.

In terms of data storage, all recognized facial features are hashed using the PBKDF2-HMAC-SHA256 algorithm and stored in encrypted form in the local Flash memory. This encryption method not only enhances data security but also ensures that even if the device is lost, the original facial data cannot be easily reconstructed. In addition, the system provides a one-click data deletion function, allowing users to permanently remove all locally stored facial data at any time, further strengthening their control over their personal information.



6. Professional Conduct and Ethics

In commercializing this face recognition robot, I would implement the following measures to uphold the highest ethical standards.

6.1. Academic Integrity

All user testing would require signed digital consent forms detailing data collection scope (facial feature vectors only), 7-day maximum retention period, and deletion protocols. Real-time data capture status would be displayed via the Micro:bit LED matrix for transparency.

End-to-end encryption would ensure facial features are immediately hashed using PBKDF2-HMAC-SHA256 after extraction, with raw image data purged from memory.Training data would exclusively use open-source datasets, avoiding copyrighted pre-trained weights.

6.2. Engineering Ethics

Hardware would integrate temperature sensors to disable the camera if the K210 chip exceeds 65°C. 3D-printed enclosures would use rounded edges to prevent assembly injuries.

Five consecutive recognition failures would trigger hibernation mode to prevent brute-force attacks, with backup battery power maintaining data wipe capability for 72 hours.

6.3. Business Ethics

All documentation would use AES-256 encryption, with employee offboarding procedures including Git history anonymization. Product packaging would state: "This device complies with open-source license. All user data ownership remains with the end-user."