Proposal

Tianze Zhang|400208135|zhant22@mcmaster.ca
Mike Zhang|400132290|zhany257@mcmaster.ca
CeZhan|400176920|zhanc63@mcmaster.ca

Executive summary

With the rising concerns surrounding security, our team is embarking on a project aimed at developing a comprehensive home security system that leverages biometric data for verification. We've aptly named our endeavor the "Biometric Homeland Security System."

Our inspiration draws from the open-source Face Recognition project on GitHub, though it's important to note that facial recognition represents just one facet of our biometric verification methods. To ensure efficient project management and milestone tracking, we've divided our project into three key deliverables.

At the Bronze level, we initiate the training process for the facial recognition mode by inputting our own faces into the training database. Concurrently, we implement three distinct scenarios for utilizing the facial recognition system, each tailored to varying distances from the camera.

Advancing to the Silver level, we enhance the system with hardware components such as a fingerprint reader and a number pad, enabling more robust biometric checks. To secure access, we integrate a step motor or solenoid lock as the system's locking mechanism.

The Gold level represents the culmination of our efforts as we seamlessly merge both software and hardware components into a compact 3D-printed enclosure. This versatile design can be readily installed on a variety of front doors, offering a comprehensive security solution.

For a deeper dive into the technical intricacies, we will provide detailed explanations in Part 4 and 5. In summary, our primary programming language for software implementation will be Python. We'll employ OpenCV-Python to operate the webcam, utilize CVZone to detect the distance between the user's face and the camera, and employ Pyserial to interface with and control the Arduino board.

Undoubtedly, the most significant challenge we anticipate is the integration of software and hardware components. Nevertheless, we are confident that our three years of dedicated study and preparation have furnished us with the necessary knowledge and expertise to effectively tackle this challenge.

Background and motivation

In today's rapidly evolving technological landscape, security concerns have driven the development of innovative products and systems aimed at safeguarding homes and personal spaces. While established market players like Google Nest, Arlo, Ring, and Eufy have made significant strides in home security, there exists a compelling opportunity to take these advancements even further.

The "Biometric Homeland Security System" project is motivated by the desire to offer homeowners an unparalleled level of security, convenience, and peace of mind. We recognize that the market currently boasts a range of security products, including smart doorbells and surveillance systems. However, we aim to set our project apart by introducing a cutting-edge home smart doorbell system that integrates multiple biometric and security features, including facial recognition, voice recognition, live feed monitoring, and automatic door lock control for homeowners.

By combining these advanced features, the "Biometric Homeland Security System" is poised to redefine the standards of home security. Our project represents a significant leap forward in technology, offering homeowners a comprehensive, intelligent, and user-friendly solution that ensures their homes remain safe and secure.

Objective

This project aims to develop an advanced facial recognition system to address the growing security needs and technological challenges. The system will combine state-of-the-art facial recognition technology and advanced algorithms to provide outstanding performance and functionality, meeting the requirements of multiple application areas.

High Accuracy Recognition: Develop a highly accurate facial recognition algorithm capable of swiftly and precisely identifying individuals under varying lighting conditions, angles, and facial expressions.

Multimodal Authentication: Implement multimodal biometric recognition, including facial recognition, voice recognition, and potentially iris or fingerprint recognition, for enhanced security.

Real-time Monitoring: Create real-time monitoring capabilities to detect and alert on irregular activities, such as unauthorized access or facial disguises.

Cross-Industry Applicability: Ensure the system is suitable for various industries, including corporate security, government applications, financial institutions, healthcare, and intelligent access control systems.

Usability and Scalability: Establish a user-friendly interface to enable administrators to easily manage and configure the system. Additionally, ensure the system's scalability to adapt to future needs and technological advancements.

Privacy and Data Security: Implement necessary privacy and data security measures to safeguard the security and compliance of personal data in accordance with relevant regulations and laws.

Project success will be demonstrated in the following ways:

- Achieving high-accuracy facial recognition meeting specified performance benchmarks.
- On-time project delivery, including comprehensive documentation and training materials.
- Completion of user satisfaction surveys to ensure the system meets user requirements.
- Effective cost control within the project budget.
- Successful collaboration within the project team to achieve project objectives.

These project objectives are designed to ensure the successful development and deployment of an advanced facial recognition system that meets diverse security and authentication needs.

Step-by-step technical approach

To comprehensively monitor the development of our system, we've devised a plan to break it down into two major components: software and hardware.

For the software aspect, we've seamlessly merged the functionality of a standard surveillance camera with facial recognition capabilities. Initially, we harnessed the power of the Face Recognition Library to process real-time camera feeds whenever a person comes into view. Subsequently, we employed libraries like OpenCV, along with CVZone, to ascertain the distance between the user and the camera. This crucial information allows us to seamlessly switch camera modes from biometric verification to regular surveillance, enabling the recording of user-defined lengths of video whenever a person enters the camera's frame. To engage users effectively, we integrated SpeechRecognition and Spacy to facilitate natural, human-like conversations with them.

As for the hardware component, we will utilize a fingerprint reader for user biometric verification, accompanied by three LED lights that serve as status indicators for the verification process. We've also implemented Pyserial for seamless communication with the main Python script, granting access to the biometric database for each user. In the event that the face recognition and fingerprint reader input match the existing database, the LED_GREEN light will illuminate, and the step motor and solenoid lock will be disengaged, allowing the user access to the front door.

To culminate this endeavor, we'll seamlessly integrate the software and hardware components into a 3-D printer case. The Raspberry Pi 4 will serve as the central hub for storing the Python script and powering the Arduino processor. Our ultimate objective is to encapsulate the entire package within a compact and portable product.

Resources

Manpower:The project is divided among the three of us, with each of us specializing in software development, hardware integration, and project management.

Knowledge and Skills: We require biometric verification, including facial recognition, fingerprint recognition, Python programming, accompanying hardware infrastructure, and database analysis and management.

Time: The planned schedule is expected to take a total of 7 months, with specific timelines for each phase. Sufficient time is allocated for research, development, testing, and integration to ensure thorough implementation.

Components:The project will require various components, including high-resolution cameras, fingerprint readers, numeric keypads, stepper motors, solenoid locks, and 3D printing materials. Additionally, software components like Python, OpenCV-Python, CVZone, and Pyserial are essential for system operation.

Budget:A budget will be allocated to cover the costs of hardware components, software licenses, research, and development efforts. The budget will also include expenses for testing, quality assurance, and potential contingencies. Excluding personnel costs, the project's material cost is approximately $200.

Schedule of activities and milestones - Project Durations: Sept. 2023 - Apr. 2024

Tentative Milestones

Project planning, define requirement and specification - late Sept.

- Review existing tech, identify hardware and software requirement
- Create system architecture

Design coding and prototyping - late Oct.

- Design the user interface
- Implement facial recognition and voice recognition algorithms
- Integrate live feed monitoring features
- Conduct thorough testing and debugging

Developments and integration with hardware - late Nov.

- Develop automatic door lock control functionality
- Built In camera, moveable camera for target tracking.
- Lighting implementation

Product testing and user feedback - Nov./Dec. With prof

- Invite beta testers to evaluate the system
- Gather user feedback on usability, security, and performance
- Make necessary adjustments based on feedback

Final project refinement and user testing - late Jan. to mid Feb. meeting with prof

- Address issues and make improvements based on beta testing
- Conduct rigorous testing for system stability and security

Complete deliverable and product presentation - late Mar.

- Prepare user manuals, documentation, and presentation
- Address any post-launch issues and improvements
- Evaluate the project's success against predefined objectives

*milestone subject to change

Risks and alternative plan

This section lists possible issues that may delay or alter the final project deliverable, and how to adjust strategy based on the issue.

Risk 1: Technology Development Challenges
Potential Risk: Developing and integrating biometric technologies like facial recognition and voice recognition may encounter technical difficulties, causing project delays.

Alternative Plan: Using pre-existing, proven biometric solutions. Conduct thorough testing early in the development phase to identify and address technical challenges promptly. If unable to follow the milestone timeline, remove project features to save development time.

Risk 2: Data Security and Privacy Concerns
Potential Risk: Concerns about data security and privacy may arise due to the nature of biometric data. This can lead to legal and regulatory challenges.

Alternative Plan: Ensure compliance with relevant data protection laws and regulations, provide user consent form, terms of agreement etc.

Risk 3: Budget Overruns
Potential Risk: Unforeseen expenses or changes in project scope can result in budget overruns.

Alternative Plan: Establish a contingency budget for unexpected expenses. Continuously monitor project expenses and make adjustments to stay within budget. Re-evaluate project scope and requirements if necessary.

Deliverables

Our project to develop a facial recognition access control system will yield several key deliverables. At theBronze level , we will kickstart the facial recognition training process by entering authorized users' facial data into the training database. Additionally, we will implement three distinct usage scenarios for the facial recognition system, each customized for different distances from the camera. Progressing to the Sliver level, we will enrich the system with supplementary hardware components, such as a fingerprint reader and a numeric keypad to enable multi-factor biometric authentication. To ensure secure access, we will integrate a stepper motor or solenoid lock as the system's locking mechanism. Finally, at the Gold level, we will seamlessly integrate both software and hardware elements into a compact 3D-printed enclosure, delivering a comprehensive and user-friendly security solution for access control.

References

Face Recognition Library (GitHub Repository) - ageitgey/face_recognition
CMake - Official Website
Dlib - Python API Documentation - dlib.net/python/index.html
OpenCV-Python (PyPI) - opencv-python
SpeechRecognition (PyPI) - SpeechRecognition
PyAudio (PyPI) - PyAudio
Computer Vision Zone - computervision.zone
MediaPipe by Google (GitHub Repository) - google/mediapipe
spaCy (Official Website) - spacy.io
pySerial (PyPI) - pyserial