Dual-Biometric Authentication System

Using ECG and Fingerprint Recognition

Joao Custodio, A47709
Anna Ghiotto, A53021

Sensores e Eletronica
January 2025

Abstract

This report presents the design and implementation of a multimodal biometric authentication system that integrates fingerprint and electrocardiogram (ECG) data for enhanced security. The system employs an Arduino and Raspberry Pi for hardware control and data processing, utilizing a fingerprint sensor to identify users and an ECG sensor to authenticate their identity based on physiological signals. An OLED display serves as the user interface, allowing for action selection between enrollment, authentication, and system reset via physical buttons.

Due to hardware limitations, the ECG sensor is non-functional, and pre-loaded ECG data is used to simulate real-time authentication under ideal conditions. Thresholds for cosine similarity are set at 0.8 for all ECG features, including R-peaks, heart rate, and filtered ECG signals, ensuring consistent authentication results in the simulation. While the system operates effectively in ideal conditions, occasional failures occur due to the low-cost hardware components, with the fingerprint sensor being particularly sensitive to dust and dirt.

The results demonstrate the feasibility of combining fingerprint and ECG data for a secure dual-authentication system. However, further testing with real ECG data and improved hardware is required to validate the system's robustness in practical scenarios. Despite these limitations, the project provides a foundation for future development of cost-effective and secure multimodal biometric systems.

Introduction

Biometrics is essential for security and individual authentication, replacing more traditional methods such as passwords or personal access tokens [1]. By using biological characteristics, it is possible to mitigate risks associated with fraud or even information theft. Biometrics encompasses both physiological and behavioral biometric data, with fingerprint recognition, categorized as physiological biometric, being the most widely used in public institutions [2] [3]. This preference is due to its ease of identification, non-transferability, and resistance to forgery.

Although biometrics is generally secure, with data typically stored in an encrypted form [2], the system can fail under certain conditions. Presentation attacks [3] may occur when someone uses another person's physical characteristics or biometric data to access a system or platform. Additionally, biometric systems are susceptible to spoofing attacks, where artificial samples (such as fake fingerprints) can deceive biometric sensors [4][3].

To better combat these types of attacks, research has proposed the use of multiple distinct biometric systems in combination, aiming to enhance user security [1]. Integrating different recognition methods creates a more robust solution, making the identification and authentication process more secure and harder to bypass. By combining different biometric features, the system increases reliability and reduces the likelihood of errors or forgery attempts, providing more effective protection against unauthorized access [5].

This method, known as multimodal authentication, lowers the risk of failure by combining data from multiple biometric sources. As a result, it achieves significantly lower false acceptance rates (FAR) and false rejection rates (FRR) compared to systems relying on a single biometric modality [2].

Despite the many advantages of multimodal biometric systems, their adoption remains limited, with estimates suggesting that only about 30% of authentication systems utilize two or more biometric modalities [1].

State of the Art and Existing Alternatives in Multimodal Biometric Systems

Multimodal biometric systems, combining fingerprint recognition and electrocardiogram (ECG) signals, are gaining attention for their enhanced security against spoofing and presentation attacks. Fingerprints provide a reliable physiological identifier, while ECG signals ensure liveness detection, addressing vulnerabilities in unimodal systems [3] [2].

Feature-level fusion, leveraging deep learning techniques like convolutional neural networks (CNNs), has demonstrated improved accuracy and robustness. Decision-level fusion, combining independent matcher outputs, is another effective approach, particularly for compatibility across diverse algorithms [2] [5]. Market alternatives include portable devices that integrate fingerprint scanners and ECG sensors for real-time, high-security applications such as border control and law enforcement [5].

However, challenges like computational complexity, processing speed, and limited multimodal datasets remain barriers to broader adoption. Overcoming these obstacles is key to unlocking the full potential of multimodal biometric systems.

Materials and Methods

Components

The following components were used in the development and implementation of the project:

1. **Elegoo Uno R3**: An Arduino-compatible microcontroller used as the primary processing unit for interfacing with sensors and peripherals. The microcontroller communicates with the Raspberry Pi via a USB-to-serial connection for transmitting and receiving data.

2. **Raspberry Pi 5**: A single-board computer employed for advanced computational tasks and handling data transmission between components.

3. **ECG Sensor (AD8232)**: Used for capturing electrocardiogram (ECG) signals to monitor cardiac activity. The sensor is connected to the Arduino as follows:

   - **Vcc**: Connected to the 3.3V pin on the Arduino.
   - **GND**: Connected to the ground (GND) pin on the Arduino.
   - **Output**: Connected to the A0 analog input pin on the Arduino.
   - **LO+ and LO-**: Not used in this setup.

   However, the ECG sensor purchased for this project was non-functional, so the system was adapted to bypass the issue by using preloaded standard ECG data. The code for acquiring real-time ECG data has been commented, and the system is designed to work with live ECG data when a functional sensor is available.

4. **Fingerprint Sensor (AS608)**: An optical sensor used for biometric identification by capturing and verifying fingerprints. The sensor is connected to the Arduino via serial communication:

   - **Vcc**: Connected to the 3.3V pin on the Arduino.
   - **GND**: Connected to the ground (GND) pin on the Arduino.
   - **TX**: Connected to digital pin 2 on the Arduino.
   - **RX**: Connected to digital pin 3 on the Arduino. The fingerprint templates are stored internally within the sensor.

5. **Breadboard**: A prototyping tool for assembling electronic circuits without soldering. It is used to interconnect the components and ensure a modular setup for testing and debugging.

6. **Connection Cables**: Male-to-male and male-to-female jumper wires are used to establish electrical connections between the microcontroller, sensors, LEDs, and other components.
7. **Resistors**: Resistors (330Ω) are used in series with the LEDs to limit the current and prevent damage to the components.
8. **Light-Emitting Diodes (LEDs)**: Connected to digital output pins on the Arduino via 330Ω resistors.
9. **Push Buttons**: Three tactile push buttons are connected to the Arduino as digital inputs. Each button corresponds to a specific system action (Enroll, Authenticate, or Exit).

These components were interconnected on the breadboard to create the circuit, with additional software implemented to ensure proper communication between the devices.

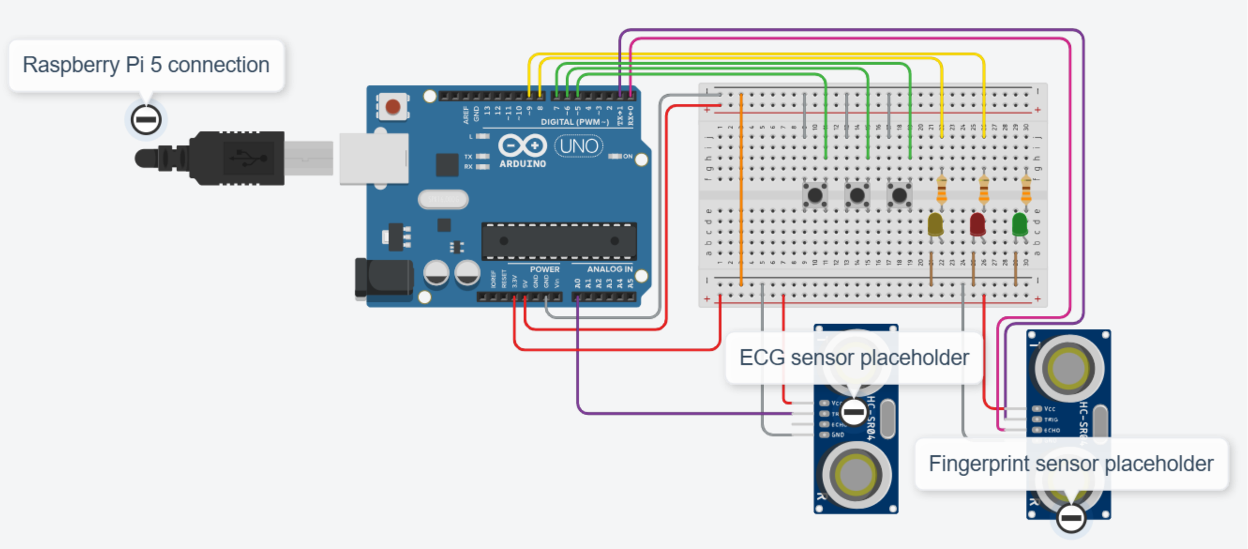

Figure 1 – Hardware connections of the biometric authentication system. The Arduino Uno interfaces with the ECG sensor (A0), fingerprint sensor (digital pins 2 and 3 for serial communication), push buttons (digital inputs), and LEDs (digital outputs with 330Ω resistors). The Raspberry Pi connects to the Arduino via USB for data processing and communication.

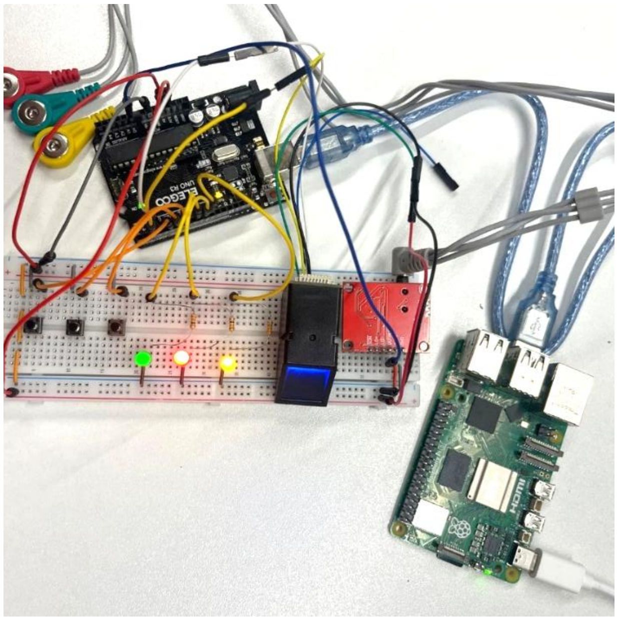

Figure 2 - Physical implementation of the biometric authentication system.

Fingerprint Sensors

Fingerprint sensors are essential devices in biometric authentication systems, utilizing the unique characteristics of the skin and finger to identify and authenticate individuals. Currently, the sensors in use operate through quite distinct methods, with the choice of the most suitable type depending on its specific application [6] [7].

Optical Sensors

Among the most well-known are optical sensors, which operate based on the principles of light refraction and reflection to generate images. The process begins when the finger comes into contact with a glass prism, where the ridges of the fingerprint absorb the light, and the valleys reflect it, creating the unique fingerprint pattern with precision. The reflected light is directed to the sensor (CMOS or CCD), which converts the light signals into electrical signals, resulting in a detailed digital image of the fingerprint, as illustrated in Figure 2 [7] [6].

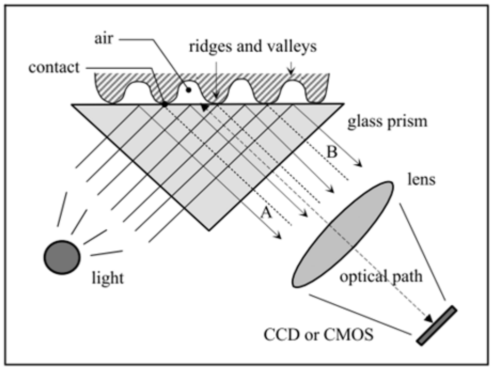

Figure 3 – Operating method of an FTIR optical sensor [7].

Optical sensors are known for being low-cost but come with some limitations. Among these is the total internal reflection (TIR) process, widely used in such sensors, which makes it difficult to miniaturize the device, thereby limiting its portability. Additionally, they are sensitive to contamination on the surface of the fingers or the sensor, which can impact image quality on dry or wet fingers and require high energy consumption [7][8]. There are already new technologies aimed at improving the performance of these sensors and mitigating their drawbacks, but currently, the cost of these improvements is too high compared to the cost of capacitive sensors [8].

ECG Sensor: AD8232

The AD8232 ECG sensor is a compact and low-power integrated signal conditioning module designed for electrocardiogram (ECG) measurement applications. It is widely used in portable and wearable health monitoring devices due to its ability to provide clear and accurate signal acquisition with minimal noise.

The AD8232 features an integrated instrumentation amplifier with a high common-mode rejection ratio (CMRR), essential for minimizing interference from external noise sources. It includes a two-pole high-pass filter to remove baseline wander and a three-pole low-pass filter to eliminate high-frequency noise, such as power-line interference. These built-in filters ensure clean ECG signal acquisition, enhancing the reliability of feature extraction for biometric authentication.

Methods

The system combines hardware and software components to enable user authentication based on fingerprint and electrocardiogram (ECG) data. The updated workflow is described below.

Initialization

At startup, the Raspberry Pi initializes the system and establishes a serial communication link with the Arduino. The Arduino signals readiness for commands by turning on all three LEDs (yellow, green, and red). The system then waits for user interaction via physical buttons connected to the Raspberry Pi.

The user selects an action by pressing one of three buttons:

- Enroll: Starts the enrollment process for a new user.
- Authenticate: Starts the authentication process for an existing user.
- Exit: Restarts the system and clears all stored data.

Enrollment Process

When the "Enroll" button is pressed, the Raspberry Pi sends an "ENROLL" command to Arduino. The yellow LED turns on, prompting the user to place their finger on the fingerprint sensor. The Arduino captures the fingerprint data and stores it internally, without transmitting it to the Raspberry Pi. Once the fingerprint is successfully stored, the yellow LED turns off.

Subsequently, the Raspberry Pi requests ECG data from the Arduino. The ECG signal is transmitted in real-time from the Arduino and processed on the Raspberry Pi using the biosppy library. This processing includes filtering the signal, detecting R-peaks, and calculating heart rate timestamps. The extracted features are saved as a JSON file on the Raspberry Pi and linked to a unique user ID. Successful enrollment is indicated by the green LED briefly illuminating. The system then returns to its idle state.

Authentication Process

When the "Authenticate" button is pressed, the Raspberry Pi sends an "AUTHENTICATE" command to the Arduino. The yellow LED turns on, prompting the user to place their finger on the fingerprint sensor. The Arduino verifies the fingerprint against its internally stored templates. If a match is found, the Arduino sends the user ID associated with the fingerprint to the Raspberry Pi. Once fingerprint verification is complete, the yellow LED turns off.

The Raspberry Pi retrieves the ECG template corresponding to the user ID and requests fresh ECG data from the Arduino. The new ECG signal is processed using the same feature extraction techniques employed during enrollment. The system compares the stored ECG template with the newly captured data using cosine similarity. Authentication results are indicated by the LEDs: if authentication is successful, the green LED turns on briefly, if authentication fails, the red LED turns on briefly.

After providing visual feedback, the system returns to its idle state.

Exit Process

When the "Exit" button is pressed, the Raspberry Pi sends an "EXIT" command to the Arduino. This triggers the deletion of all stored data: the Raspberry Pi deletes all ECG templates, and Arduino erases all fingerprint models from its internal storage.

Both devices then restart automatically. Upon restarting, the system returns to its initial state, with all three LEDs (yellow, green, and red) illuminated to indicate readiness for new user interaction.

Results

The developed system successfully authenticates users based on fingerprint and ECG data under ideal conditions. User enrollment and authentication are reliably performed when hardware components operate as intended. With cosine similarity thresholds set at 0.8 for R-peaks, heart rate, and filtered ECG signal, authentication using pre-loaded ECG data consistently succeeds in simulated conditions.

Hardware limitations occasionally affect reliability. The fingerprint sensor works effectively when clean but is sensitive to dust and smudges, while the damaged ECG sensor necessitates the use of pre-loaded data. Physical buttons and LED indicators provide intuitive and consistent user interaction, with yellow, green, and red LEDs signaling fingerprint interaction, successful operations, and failures, respectively. Despite these limitations, the system effectively performs enrollment, authentication, and reset functions under controlled conditions.

Discussion

The system demonstrates the potential of multimodal biometric authentication, combining fingerprint and ECG data to enhance security. Testing with pre-loaded ECG data under ideal conditions highlights the system's feasibility but does not account for real-world variability in ECG signals. A functional ECG sensor would enable evaluation under realistic scenarios, where factors such as physiological conditions, electrode placement, and signal noise may impact reliability.

Cosine similarity thresholds were set at 0.8 for R-peaks, heart rate, and filtered ECG signals to minimize false negatives in ideal conditions. While effective, future work should optimize these thresholds to balance security and reliability in practical applications.

Low-cost hardware introduces limitations, such as the fingerprint sensor's sensitivity to dust and the damaged ECG sensor, which prevented live data testing. Despite these issues, physical buttons and LED indicators provided generally reliable user interaction.

This dual-authentication approach demonstrates significant security benefits by requiring both biometric inputs, reducing the risk of unauthorized access. Future improvements should include testing with a functional ECG sensor, optimizing thresholds, and incorporating higher-quality components to enhance system robustness and reliability for real-world applications.

Conclusion

The biometric authentication system successfully integrates fingerprint and ECG data, demonstrating reliable enrollment and authentication under ideal simulated conditions. With cosine similarity thresholds set at 0.8 for R-peaks, heart rate, and filtered ECG signals, the system balances minimizing false negatives with reliable performance in controlled tests.

However, the reliance on simulated ECG data due to a damaged sensor and occasional failures of low-cost components, such as the fingerprint sensor, highlight areas for improvement. Enhancing hardware reliability, replacing the ECG sensor, and testing with real user data are critical for evaluating and optimizing the system's performance under realistic conditions.

Future efforts should focus on optimizing similarity thresholds, improving component quality, and conducting extensive testing to refine the system's robustness. Despite these challenges, the system provides a solid foundation for developing secure and practical multimodal biometric authentication solutions.

References

[1] A. Al Abdulwahid, N. Clarke, I. Stengel, S. Furnell, e C. Reich, «Continuous and transparent multimodal authentication: reviewing the state of the art», *Cluster Comput*, vol. 19, n. 1, pp. 455–474, Mar. 2016, doi: 10.1007/s10586-015-0510-4.

[2] M. B. E, A. M. Abhishek, e H. Professor, «Multimodal Biometric Authentication using ECG and Fingerprint L M Patnaik», 2015.

[3] N. Ammour, Y. Bazi, e N. Alajlan, «Multimodal Approach for Enhancing Biometric Authentication», *J Imaging*, vol. 9, n. 9, Set. 2023, doi: 10.3390/jimaging9090168.

[4] M. Komeili, N. Armanfard, e D. Hatzinakos, «Liveness Detection and Automatic Template Updating Using Fusion of ECG and Fingerprint», *IEEE Transactions on Information Forensics and Security*, vol. 13, n. 7, pp. 1810–1822, Jul. 2018, doi: 10.1109/TIFS.2018.2804890.

[5] J. S. Arteaga-Falconi, H. Al Osman, e A. El Saddik, «ECG and fingerprint bimodal authentication», *Sustain Cities Soc*, vol. 40, pp. 274–283, Jul. 2018, doi: 10.1016/j.scs.2017.12.023.

[6] Y. Yu, Q. Niu, X. Li, J. Xue, W. Liu, e D. Lin, «A Review of Fingerprint Sensors: Mechanism, Characteristics, and Applications», 1 de Junho de 2023, *MDPI*. doi: 10.3390/mi14061253.

[7] A. J. Mohamed Abdul Cader, J. Banks, e V. Chandran, «Fingerprint Systems: Sensors, Image Acquisition, Interoperability and Challenges», *Sensors*, vol. 23, n. 14, Jul. 2023, doi: 10.3390/s23146591.

[8] Lunji Qiu, *Fingerprint sensor technology*. IEEE, 2014.

[9] M. Ingale, R. Cordeiro, S. Thentu, Y. Park, e N. Karimian, «ECG Biometric Authentication: A Comparative Analysis», *IEEE Access*, vol. 8, pp. 117853–117866, 2020, doi: 10.1109/ACCESS.2020.3004464.