STUDENT AUTHENTICATION USING FINGERPRINT SENSOR

Khushi Gupta(1RV22CS084), Lahari R(1RV22CS094), Manasa S(1RV22CS105), Posam Harshitha(1RV22CS139)

Department of Computer Science and Engineering
RV College of Engineering, Bangalore - 560059, INDIA

Go, change the world

MOTIVATION:

In educational institutions, ensuring the security of access to sensitive areas, such as classrooms, laboratories, libraries, and examination centers, is of paramount importance. Traditional methods of access control, such as keys or ID cards, have limitations in terms of security and convenience. Therefore, there is a need for a robust and efficient student authentication system.The problem at hand is to develop a student authentication system that leverages biometric technology, specifically fingerprint recognition, to enhance security and streamline access control within the educational environment.

What is a Fingerprint sensor with RTC module?

In a student authentication system using a fingerprint sensor integrated with an RTC (Real-Time Clock) module, these components work in tandem to provide secure and time-sensitive access control.The fingerprint sensor serves as the primary means of user authentication. When a student seeks access to a specific area or service within an educational institution, they place their finger on the fingerprint sensor. The sensor captures and analyzes the unique fingerprint patterns of the student, comparing them to pre-stored fingerprint templates in the system's database. If a match is found, access is granted.The RTC module plays a pivotal role in enhancing the functionality and security of the system. It maintains accurate timekeeping independently, often backed by a battery, ensuring that it continues to operate even if the main power source is temporarily disrupted. The RTC module provides precise date and time information.

WORKING

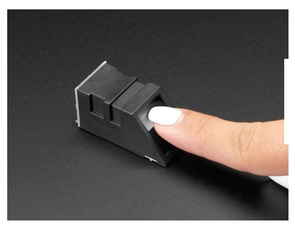
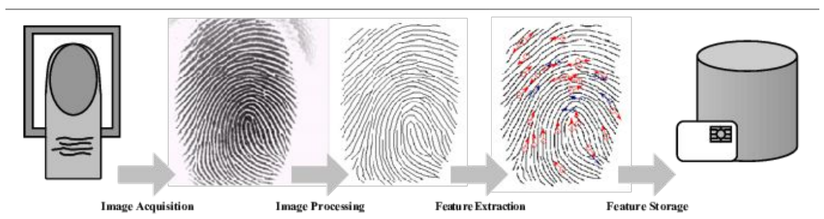
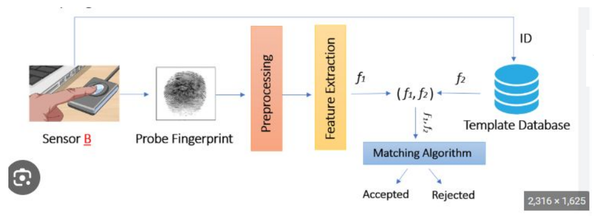


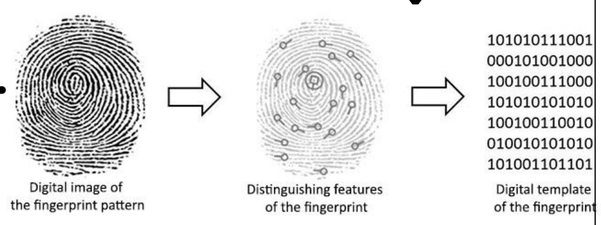
IMAGE CAPTURE: When a user places their finger on the sensor, the R307 module captures an image of the fingerprint using an array of small sensors and is stored in the form of **digital representation.**



FEATURE EXTRACTION:

The captured fingerprint image is then processed to extract **specific features** that are unique to the fingerprint, such as ridge endings, bifurcations and can be easily compared or matched.





Template Creation:

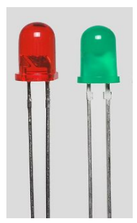
The extracted features are used to **generate a template,** which is a mathematical representation of the fingerprint and id stored .

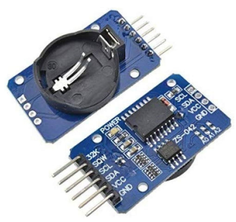
Matching

This newly generated template is then compared to the stored templates in the module's memory. If there is a **close match** between the newly generated template and any of the stored templates, the user is authenticated.

Components Used:

1.Arduino Uno
2.RTC Module
3.307 FingerPrint Sensor
4.leds
5.buzzer





RESULT:

1. Enrolling a fingerprint as ID 14.

```
12:10:25.561 -> .
12:10:25.831 -> .
12:10:26.115 -> Image taken
12:10:26.630 -> Image converted
12:10:26.675 -> Remove finger
12:10:28.749 -> ID 14
12:10:28.749 -> Place same finger again
12:10:29.031 -> .Image taken
12:10:29.881 -> Image converted
12:10:29.881 -> Creating model for #14
12:10:29.913 -> Prints matched!
12:10:29.913 -> ID 14
12:10:29.946 -> Stored!
12:10:29.980 -> Ready to enroll a fingerprint!
12:10:29.980 -> Please type in the ID # (from 1 to 127) you want to save this finger as...
```

2. Matching the fingerprint with the existing one

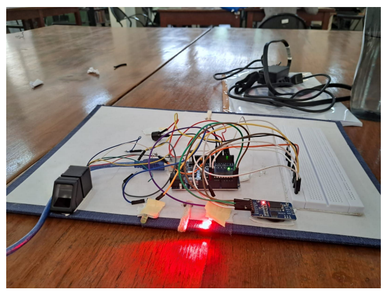
```
12:12:33.263 -> No finger detected
12:12:35.433 -> Image taken
12:12:35.993 -> Image converted
12:12:36.102 -> Found a print match!
12:12:36.134 -> Found ID #14 with confidence of 162
```

3. Deleting a single fingerprint

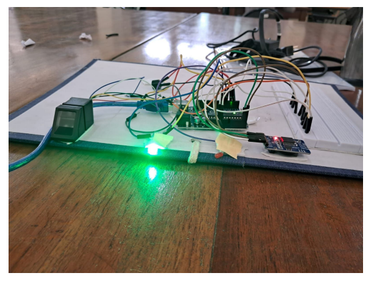
```
12:13:57.586 -> Delete Finger
12:13:58.614 -> Found fingerprint sensor!
12:13:58.614 -> Please type in the ID # (from 1 to 127) you want to delete...
12:14:26.651 -> Deleting ID #5
12:14:26.683 -> Deleted!
12:14:26.718 -> Please type in the ID # (from 1 to 127) you want to delete...
```

CONCLUSION:

In conclusion, the "Student Authentication Using Fingerprint Sensor and RTC Module" project has successfully achieved its objectives by creating a robust and innovative solution for enhancing security and access control within educational institutions. Through the integration of the fingerprint sensor, we have established a highly secure and personalized means of student identification, mitigating the vulnerabilities associated with traditional access methods. Furthermore, the incorporation of the RTC module has empowered the system with time-based access control, allowing for efficient management of access schedules, particularly in classrooms, labs, and libraries. This project not only fulfills its immediate purpose but also opens the door to future enhancements and applications in educational settings. Overall, the system's effectiveness in bolstering security and its potential for scalability make it a valuable asset for educational institutions seeking to create a safer, more efficient, and technologically advanced learning environment.



When fingerprint is not matched.



When fingerprint is matched.

REFERENCES:

1.Nguyen, H. T, “Fingerprints classification through image analysis and machine learning method”. Algorithms, vol. 12, no. 11, 2019.
2.Darlow. L. and Rosman. B, “Fingerprint minutiae extraction using deep learning”. In Proc. IEEE IJCB, 2017.
3.Salakhutdinov, R., Tenenbaum, J. B, & Torralba, A, "Learning with hierarchical-deep model," IEEE transactions on pattern analysis and machine intelligence, vol. 35, no. 8, pp. 1958-1971, 2012.
4.Deng, L., He, X., & Gao, J, “Deep stacking networks for information retrieval”, In Proc. IEEE International Conference on Acoustics, Speech and Signal Processing, pp. 3153-3157, IEEE, 2013

Guide Information:

Dr. Jayalatha(Dept of Mathematics),Dr. Avadhani(Dep tOf Physics),Dr. Pavithra H(Dept of CSE) and Dr. Pandry Narendra Rao(Dept of Electrical Engineering) RVCE.

Khushi Gupta-1RV22CS084
Lahari R-1RV22CS094
Manasa S-1RV22CS105
Posam Harshitha-1RV22CS139