

Biometric Door Lock System

Pushparani M K¹, Bindu S V², Vandana V³, Nivaas M⁴, Yashwanth D S⁵

Associate Professor, Department of CSD¹

Students, Department of CSD²⁻⁵

Alvas Institute of Engineering & Technology, Mangalore, India

Abstract: *Biometric door lock systems represent a significant advancement in security technology by utilizing unique physiological and behavioral characteristics of individuals for access control. Security and convenience are becoming increasingly important in everyday life, especially for home and office access. One popular solution uses fingerprints to unlock doors, allowing only authorized users to enter. This review looks at how fingerprint door lock systems work, including how they scan, store, and match fingerprints. It also discusses the benefits, like ease of use and better protection compared to traditional locks, as well as challenges such as sensor issues and the risk of fake fingerprints. Recent improvements in technology and ideas for making these systems even better in the future are also explored.*

Keywords: In Fingerprint recognition, biometric security, door lock system, access control, spoofing, fingerprint sensor, authentication

I. INTRODUCTION

Keeping our homes, offices, and buildings safe is very important. Traditional locks and keys have been used for a long time, but they can be lost, stolen, or copied. Because of this, many people are now using biometric systems that use parts of the human body, like fingerprints, for better security. Fingerprint door lock systems are one of the most common types of biometric security. They work by scanning a person's fingerprint and checking if it matches the one saved in the system. If it matches, the door unlocks. Since every person has a unique fingerprint, this method is both safe and easy to use. This paper gives an overview of how fingerprint door lock systems work, their benefits, problems, and how they are being improved with new technology. It also looks at where these systems are used and what the future might hold for them.

II. FINGERPRINT RECOGNITION TECHNOLOGY

An easy way to comply with the Journal paper formatting requirements is to use this document as a template and simply type your text into it.

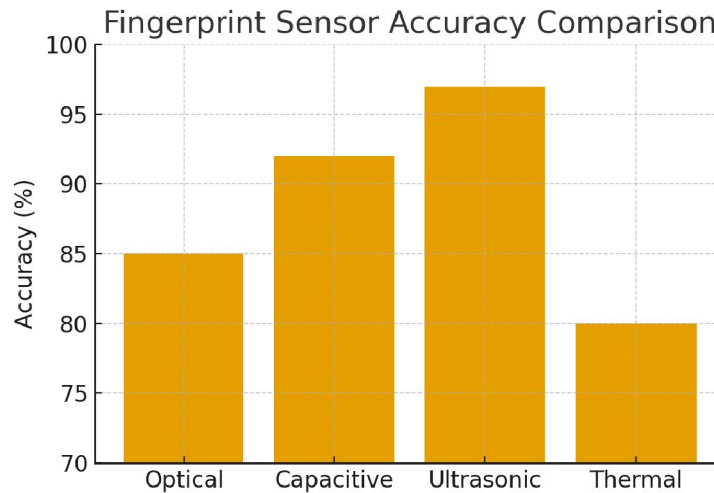
A. Fingerprint Characteristics

- Ridge patterns and minutiae points (ridge endings, bifurcations) form the basis of identification.
- Universality: nearly all humans possess unique fingerprints.
- Permanence: patterns remain consistent throughout a person's life.

B. Sensing Technologies

- Optical sensors: capture 2D fingerprint images using light reflection.
- Capacitive sensors: detect electrical properties of ridges and valleys.
- Ultrasonic sensors: use high-frequency sound waves for 3D imaging.
- Thermal sensors: detect heat patterns from finger ridges.

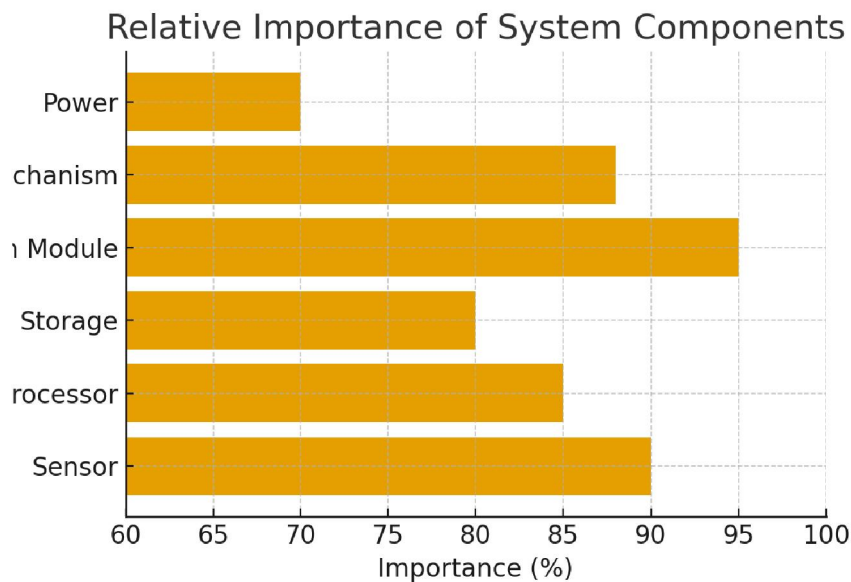




III. SYSTEM ARCHITECTURE OF FINGERPRINT DOOR LOCKS

A typical fingerprint-based door lock includes:

1. Fingerprint Sensor – captures the fingerprint image.
2. Microcontroller/Processor – extracts features and performs matching.
3. Template Storage – stores encrypted fingerprint templates.
4. Authentication Module – compares live input with stored templates.
5. Locking Mechanism – electromechanical system (e.g., solenoid, deadbolt).
6. Power Unit – battery supply, sometimes with backup options.



Advantages and Limitations

Advantages:

- High security compared to keys, PINs, or RFID cards.
- Convenience: quick access without carrying physical tokens.
- Difficult to duplicate fingerprints.
- Scalable: can register multiple users.
- Provides audit trail for monitoring access.

Limitations:

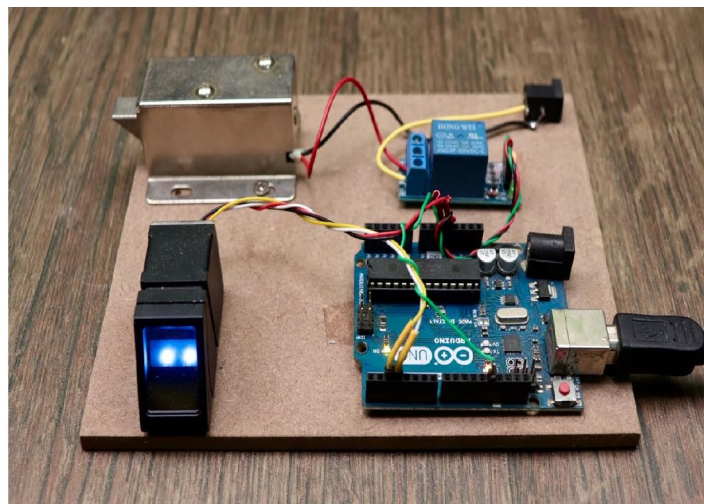
- Spoofing: fake fingerprints made from silicone, gel, or prints left on surfaces.
- Sensor issues: dirty, wet, or injured fingers may cause authentication failures.
- False Acceptance Rate (FAR) and False Rejection Rate (FRR): performance trade-off between security and convenience.
- Cost: though decreasing, high-quality sensors remain more expensive than traditional locks.
- Privacy: risk of biometric data misuse if templates are not securely stored.

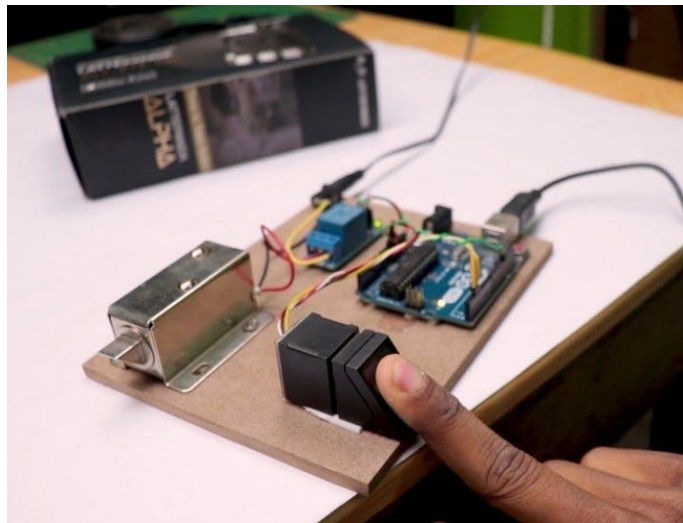
Applications

- Residential homes: replacing mechanical locks with smart, keyless entry.
- Corporate offices: restricting access to secure areas.
- Educational institutions: access control in labs or hostels.
- Healthcare facilities: securing restricted rooms (e.g., pharmacies, labs).

Future Trends

- AI-enhanced fingerprint recognition: deep learning to improve accuracy and spoof detection.
- Integration with IoT/Smart Homes: remote monitoring via mobile applications.
- Multimodal biometrics: combining fingerprint with face or voice for enhanced security.
- Blockchain-based storage: ensuring secure, tamper-proof biometric data management.
- Energy-efficient sensors: enabling long-term, battery-powered operation





D. Links and Bookmarks

- Patent: <http://patents.google.com/patent/US20030141959A1/en>
- Patent: <http://patents.google.com/patent/US7023319B2/en>
- Website: <http://www.instructables.com/Biometric-Door-Lock-Security-System-Using-Arduino>

IV. CONCLUSION

Fingerprint door lock systems are a modern and easy way to keep places safe. They use each person's unique fingerprint, which makes it hard for others to get in without permission. These systems are better than keys because you can't lose or forget your fingerprint. Even though there are some small problems, like sensor errors or fake fingerprints, new technology is helping to fix them. In the future, fingerprint locks will likely become even more common and better. They are a good choice for anyone looking for simple, fast, and safe security.

V. ACKNOWLEDGMENT

I would like to thank my guide/teacher Pushparani M K for their valuable support and guidance throughout this work. I am also grateful to my institution, Alvas Institute of Engineering and Technology, for providing the resources and environment needed to complete this review. Finally, I appreciate the encouragement and help from my friends and family during the writing of this paper.

REFERENCES

- [1] A. K. Jain, L. Hong, S. Pankanti, and R. Bolle, "An Identity-Authentication System Using Fingerprints," *Proceedings of the IEEE*, vol. 85, no. 9, pp. 1365-1388, Sep. 1997.
- [2] D. Maltoni, D. Maio, A. K. Jain, and S. Prabhakar, *Handbook of Fingerprint Recognition*, 2nd ed. New York, NY, USA: Springer, 2009.
- [3] M. Ratha, J. Connell, and R. Bolle, "Enhancing security and privacy in biometrics-based authentication systems," *IBM Systems Journal*, vol. 40, no. 3, pp. 614-634, 2001.
- [4] S. Uludag, S. Pankanti, S. Prabhakar, and A. K. Jain, "Biometric cryptosystems: issues and challenges," *Proceedings of the IEEE*, vol. 92, no. 6, pp. 948-960, Jun. 2004.
- [5] R. Kumar and K. R. Babu, "Design and Implementation of Fingerprint-Based Door Lock System," *International Journal of Advanced Research in Electrical, Electronics and Instrumentation Engineering*, vol. 4, no. 5, pp. 4272-4277, May 2015.

