

VEHICLE – SMART ENGINE LOCK SYSTEM USING BIOMETRIC AUTHENTICATION: FACE RECOGNITION AND FINGERPRINT

Interim Report Presentation

Name : M. R. M. Rashid
Field : Automotive
Engineering
Registration No. : M19940405007



Introduction



Background

- Vehicle security is a growing concern due to increasing car thefts.
- Traditional security methods (keys, PINs) are vulnerable to hacking.
- Biometric authentication offers a secure and convenient alternative.
- This project focuses on integrating face recognition and fingerprint scanning for vehicle authentication.

Objectives

- Enhance Vehicle Security
- Create a Seamless User Experience
- Create a Scalable Solution is to offer for different vehicle types
- Foster Market Innovation

Methodology

1. Literature Review: Study biometric applications in vehicle security.
2. System Design: Develop face recognition and fingerprint authentication modules.
3. Hardware & Software Integration: Implement sensors, cameras, and security protocols.
4. Prototype Development: Build a working model for testing.
5. Testing & Debugging: Validate system reliability and security.

Limitations

- Environmental factors (lighting, weather) affecting face recognition.
- Cost of implementation in existing vehicles.
- Privacy concerns regarding biometric data storage.
- Risk of biometric spoofing (e.g., fake fingerprints or photos).



Literature Reveiw

Vehicle Security Challenges



- Key-based systems: Can be stolen or duplicated.
- RFID & Key Fobs: Prone to relay attacks and hacking.
- PIN & Passwords: Susceptible to shoulder surfing and brute force attacks.

references

- Uses unique biological traits for identification.
- Common methods: Fingerprint, face, iris, and voice recognition.
- Benefits: High security, convenience, and difficult to forge.

references

What is Biometric authentication?



Face Recognition in Vehicles

references



- Uses a camera to scan and analyze facial features.
- AI algorithms compare the image with pre-registered data.
- Works even in low-light conditions using infrared sensors.
- Hands-free and convenient access method



Fingerprint Recognition in Vehicles

references

- Captures fingerprint pattern using a scanner.
- Compares with stored biometric data for verification.
- Integrated into dashboard, door handles, or ignition panels.
- Provides quick and reliable authentication.

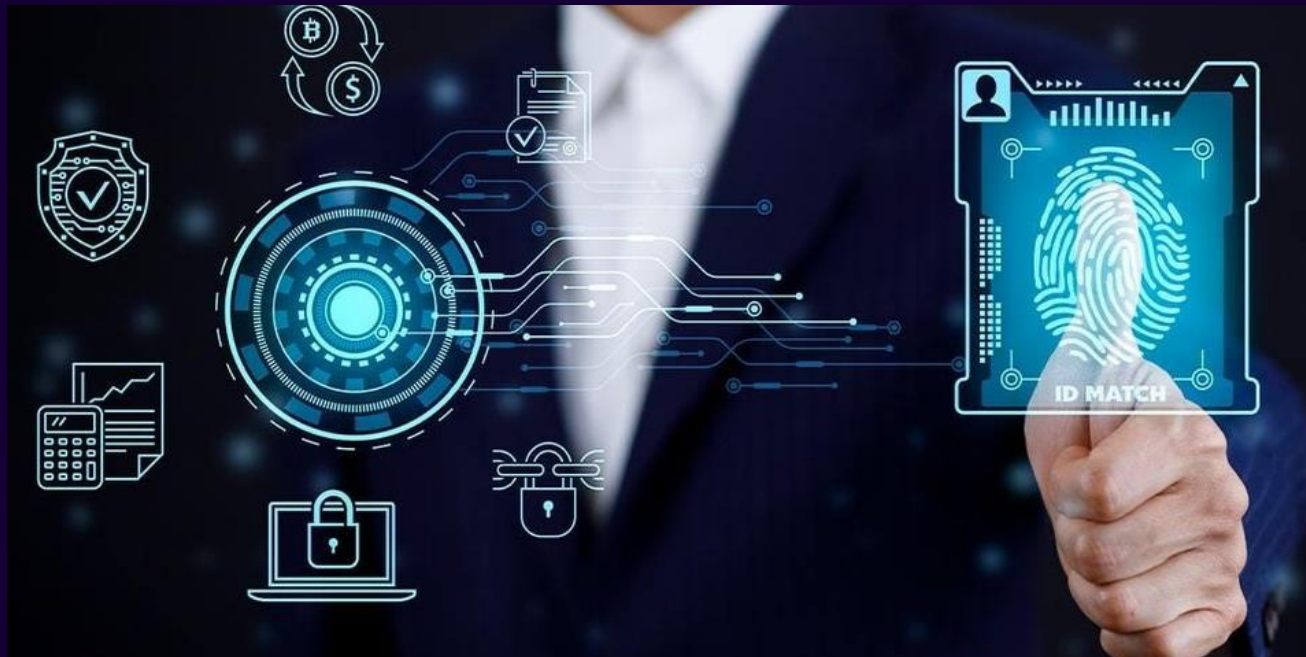
- Combining multiple biometric methods for enhanced security.
- Example: Face + Fingerprint Authentication.
- Reduces false positives and improves reliability.

references

Multifactor Authentication



Advantages of Biometric Authentication



- ✓ High Security – Unique biological traits prevent duplication.
- ✓ Convenience – No need to remember PINs or carry keys.
- ✓ Speed – Instant authentication reduces wait time.
- ✓ User Personalization – Adjusts settings for different drivers.
- ✓ Difficult to Hack – Unlike passwords or RFID, biometrics cannot be easily stolen

references

- ✗ Costly Implementation – Advanced hardware and software required.
- ✗ Privacy Concerns – Secure biometric data storage needed.
- ✗ Environmental Sensitivity – Face recognition may fail in poor lighting.
- ✗ Biometric Spoofing – Risk of fake fingerprints or facial images being used.

references

Limitations of Biometric Authentication



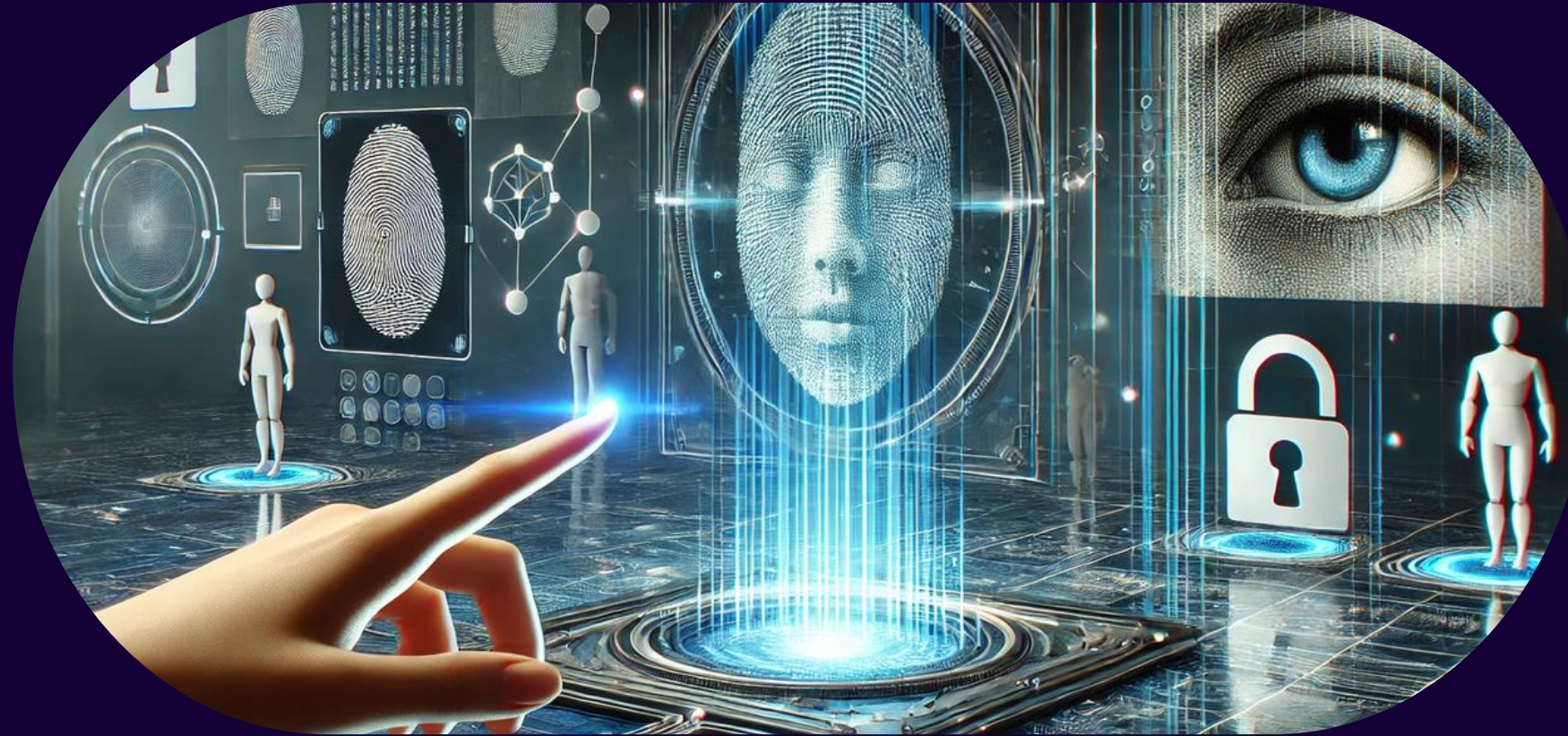
Future of Biometric Vehicle Security



- AI-Powered Recognition – Improved accuracy with machine learning.
- Iris & Voice Authentication – Additional biometric layers for security.
- Cloud-Based Authentication – Secure storage and real-time verification.
- Integration with Autonomous Vehicles – Seamless access and personalization.

references

Conclusion



- Biometric authentication enhances vehicle security and user convenience.
- Face & Fingerprint Recognition provide a multi-layered defense system.
- Challenges exist (cost, privacy, environmental factors), but advancements continue.
- Future innovation will make biometric vehicle security more reliable and widespread.

Thank you
for your
attention
and support!

