International Journal of Scientific Research in Engineering and Management (IJSREM)
Volume: 09 Issue: 05 | May - 2025 SJIF Rating: 8.586 ISSN: 2582-3930

AI-Driven Facial Recognition System for Secure and Efficient Bike Starter Authentication Using Machine Learning

Dr Kamalakannan S
Associate Professor, Dept. Of ECE,
KGiSL Institute of Technology
Coimbatore, TN, India
kamalsphd@gmail.com

Hemapriya T
UG Student, Dept. Of ECE,
KGiSL Institute of Technology
Coimbatore, TN, India
hemapriya3751@gmail.com

Hariharan R
UG Student, Dept. Of ECE,
KGiSL Institute of Technology
Coimbatore, TN, India
hariravi2003r@gmail.com

Eswari K
UG Student, Dept. Of ECE,
KGiSL Institute of Technology
Coimbatore, TN, India
eswarikalaignan@gmail.com

Hari M
UG Student, Dept. Of ECE,
KGiSL Institute of Technology
Coimbatore, TN, India
harimurugan.m17@gmail.com

Mohammed Mahboob Basha S.M
UG Student, Dept. Of ECE,
KGiSI Institute of Technology
Coimbatore, TN, India
mohammedmahboob2006@gmail.com

ABSTRACT

With the rise of smart technology, integrating facial recognition into vehicle security systems is becoming increasingly popular. This project aims to develop a Face Recognition-Based Bike Starter System to enhance bike security and prevent unauthorized access. The system employs a camera module to capture the rider's face and compares it with a pre-registered database using AI-based facial recognition algorithms. If authentication is successful, the system triggers the bike's ignition system; otherwise, access is denied.

The proposed system uses OpenCV for image processing, a Raspberry Pi/Arduino for processing, and a relay module to control the ignition. Additionally, it can be enhanced with cloud storage for remote monitoring and mobile app integration for user convenience. The implementation of this technology significantly reduces the risk of theft compared to traditional key-based mechanisms.

By leveraging advanced biometric authentication, this project introduces a secure, efficient, and user-friendly bike-starting mechanism. It represents a step forward in automotive security, blending AI, IoT, and embedded systems to provide a smart solution for modern-day /transportation challenges.

Keywords - Face Recognition, AI-based Authentication, OpenCV, Raspberry Pi, IoT,

I. INTRODUCTION

In today's world, vehicle theft is a major concern, with traditional key-based ignition systems being vulnerable to duplication or unauthorized access. To address this issue, modern security systems are integrating biometric authentication, which offers a more secure and convenient alternative. Among various biometric methods, facial recognition stands out due to its non-intrusive nature, accuracy, and ease of use. This project aims to develop a Face Recognition-Based Bike Starter System, which enhances security by ensuring that only authorized users can start the bike.

The proposed system utilizes a camera module to capture the rider's face and compare it with a pre-stored database using artificial intelligence (AI) and image processing algorithms. If the system recognizes the face, it sends a signal to the ignition control unit to start the bike; otherwise, access is denied. The system is implemented using OpenCV for facial recognition, Raspberry Pi/Arduino as the processing unit, and a relay module to control the ignition. Additionally, it can be extended with cloud storage for remote access and a mobile app for user authentication and alerts.

This face recognition-based system offers several advantages over conventional methods. Unlike keys or PIN-based systems, facial recognition eliminates the risk of theft due to key duplication or unauthorized access. It also enhances user convenience by providing a keyless ignition system that operates seamlessly. Furthermore, it can be integrated with IoT-based security systems to notify the owner of unauthorized access.

With the increasing advancements in AI and embedded systems, implementing facial recognition in vehicles represents a significant step toward smart and secure transportation solutions. This project not only strengthens bike security but also showcases the potential of biometric authentication in the automotive industry, paving the way for future innovations.

II. LITERATURESURVEY

The integration of biometric authentication in vehicle security systems has been a topic of extensive research in recent years. Traditional bike security mechanisms, such as key-based and RFID- based systems, are prone to theft and unauthorized duplication. To overcome these limitations, researchers have explored facial recognition technology as a secure and reliable alternative.

Several studies have been conducted on face recognition-based security systems. OpenCV-based facial detection techniques, combined with machine learning algorithms such as Haar Cascades, LBPH (Local Binary Pattern Histogram), and deep learning models like CNN (Convolutional Neural Networks), have demonstrated high accuracy in real-time facial recognition. A study by Viola and Jones (2001) introduced a robust face detection algorithm, which remains a foundation for modern real-time recognition systems. Raspberry Pi-based authentication systems for vehicle security, using camera modules for real- time face detection and verification. These studies indicate that Raspberry Pi, in combination with Python-based OpenCV libraries, can effectively recognize faces with minimal processing delay. Additionally, Arduino-controlled ignition systems have been explored for implementing smart locks and keyless entry mechanisms.

Recent advancements have also highlighted the role of cloud storage and IoT integration in security systems, enabling remote access and monitoring. Studies have proposed real-time notifications to alert owners about unauthorized access attempts, further enhancing vehicle safety.

Despite the progress, challenges such as low-light recognition, image spoofing, and processing speed remain areas of ongoing research. This project builds upon previous works by integrating AI-driven face recognition, embedded system control, and IoT-based remote monitoring to develop a secure and efficient bike ignition system, reducing theft risks and enhancing user convenience.

Thus, this literature survey establishes the feasibility and significance of implementing a face recognition-based bike starter system as a next- generation vehicle security solution.

III. METHODOLOGY

The Face Recognition Bike Starter system utilizes advanced computer vision and machine learning techniques to enhance vehicle security. The methodology begins with data collection and preprocessing, where a high-resolution camera captures facial images of authorized users. These images undergo preprocessing steps such as grayscale conversion, noise reduction, and normalization to enhance recognition accuracy. Next, a deep learning-based facial recognition model, such as OpenCV's LBPH or a neural network using TensorFlow, is developed and trained with multiple images to ensure reliable authentication. The system is then integrated with a microcontroller, such as Raspberry Pi or Arduino, which connects the facial recognition module to the bike's ignition system. When a face is detected, the system extracts facial features and compares them with stored data. If a match is found, the ignition is activated; otherwise, access is denied. To enhance security, encryption techniques are implemented to prevent unauthorized access, while real-time processing optimizations ensure quick authentication. The final stage involves rigorous testing under various lighting and environmental conditions to validate accuracy and reliability, making necessary adjustments before deployment. This methodology ensures a secure and efficient facial recognition- based bike ignition system, reducing the risk of theft while enhancing user convenience.

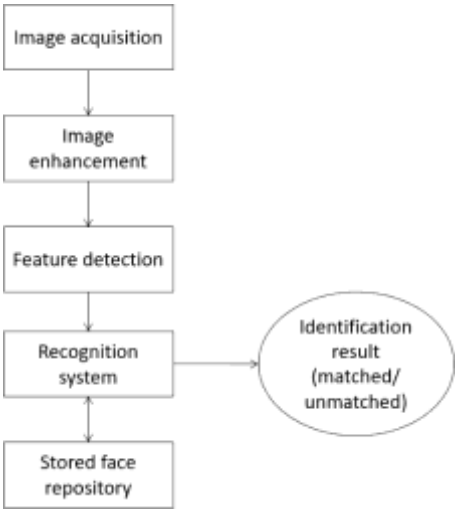
IV. EXISTING SYSTEM

The existing bike ignition systems primarily rely on physical keys, RFID-based keyless entry, or numerical passcodes for security. The most common method involves using a physical key, but this poses a high risk of theft due to key duplication, loss, or unauthorized access. Some modern bikes incorporate RFID or smart key systems, which offer improved security but remain vulnerable to hacking

or signal interception. In recent years, biometric authentication, such as fingerprint recognition, has been introduced in high-end vehicles, but this method is often affected by environmental factors like dirt, moisture, and sensor wear, leading to reduced reliability. Another emerging approach is mobile app-based authentication, where users can start their bike using a Bluetooth-connected smartphone application. While convenient, this method introduces risks such as hacking, phone theft, or connectivity issues. Despite these advancements, existing systems still rely on physical or digital keys, making them susceptible to unauthorized access and theft. Additionally, they often lack multi-layered security features and require user intervention, such as inserting a key, entering a passcode, or using a mobile device, which may be inconvenient in certain situations. Due to these limitations, there is a growing need for a more advanced and secure bike ignition system. Face recognition technology offers a promising alternative by providing a seamless, hands-free authentication process that enhances security while ensuring convenience for the rider.

V. PROPOSED SYSTEM

The Face Recognition Bike Starter system is an advanced security solution designed to provide a keyless and hands-free ignition method using facial recognition technology. This system eliminates the need for traditional keys, RFID cards, or mobile authentication, reducing the risk of theft and unauthorized access. A high-resolution camera installed on the bike's dashboard captures the rider's face in real-time. The captured image undergoes preprocessing, including grayscale conversion, feature extraction, and normalization, to enhance accuracy. A deep learning-based facial recognition model, such as OpenCV's LBPH or a convolutional neural network (CNN), compares the captured face with stored images of authorized users. If a match is found, a microcontroller, such as a Raspberry Pi or Arduino, sends a signal to the bike's ignition system, allowing the engine to start. If the system detects an unauthorized user, access is denied, preventing the bike from starting. To enhance security, encryption techniques are applied to store and protect user facial data from hacking attempts. Additionally, real-time processing optimizations, such as edge computing, ensure quick and efficient authentication. The system is designed to function reliably under different lighting and environmental conditions, making it suitable for everyday use. By eliminating the need for physical keys and digital passcodes, this proposed system significantly enhances security while offering a seamless and modern approach to bike ignition.



VI. WORKING OF PROPOSED SYSTEM

The Face Recognition Bike Starter system operates through a series of well-defined steps that ensure a secure, efficient, and convenient bike ignition process using facial recognition technology. This system eliminates the need for traditional keys, RFID cards, or mobile-based authentication, reducing the risk of theft and unauthorized access. The working of the system involves several stages, including image acquisition, facial recognition, authentication, and ignition control.

1. Image Acquisition and Preprocessing

When the rider approaches the bike, a high-resolution camera installed on the bike's dashboard captures the rider's face in real-time. The camera continuously scans for a human face within a predefined range. Once a face is detected, the image undergoes preprocessing to enhance recognition accuracy. This involves grayscale conversion, noise reduction, histogram equalization, and feature extraction. These processes improve the clarity of the captured image and reduce external factors such as shadows and background noise.

2. Facial Recognition and Authentication

After preprocessing, the system employs a deep learning-based facial recognition model, such as OpenCV's LBPH (Local Binary Patterns Histogram) or a convolutional neural network (CNN), to analyze the unique facial features of the captured image. The extracted features are

compared with the stored facial data of authorized users in the system's database. If a match is found, authentication is successful, and the system proceeds to the next step. If the detected face does not match any authorized user, access is denied, and the bike remains locked.

3. Ignition Control Mechanism

Once the system successfully authenticates the rider, a microcontroller—such as a Raspberry Pi or Arduino—sends a signal to the bike's ignition system, allowing the engine to start. This process occurs almost instantly, ensuring a seamless and hassle-free experience for the user. If the face is not recognized or unauthorized access is attempted multiple times, the system can trigger an alert mechanism, such as sending a notification to the owner's mobile device or activating an alarm to deter potential theft.

4. Security Measures and Data Protection

To enhance security, the system integrates encryption techniques to protect stored facial data, preventing hacking or unauthorized modifications. The facial recognition model is designed to work efficiently even under different lighting conditions, such as low-light environments or bright sunlight, by dynamically adjusting brightness and contrast settings. Additionally, the system incorporates anti-spoofing mechanisms to prevent unauthorized access using photos, videos, or 3D masks.

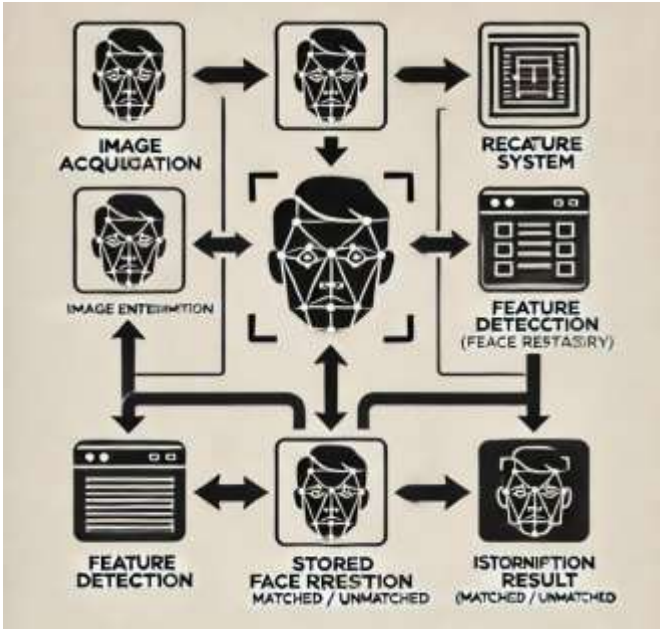
5. Fail-Safe Mechanisms and Backup Options

In case of camera failure, poor lighting, or technical issues, the system includes an override mechanism that allows manual unlocking through a mobile app or a security PIN. This ensures that the rider is not left stranded if the facial recognition system is temporarily unavailable.

6. Real-Time Processing and Performance Optimization

To provide a fast and efficient user experience, the system implements real-time processing techniques such as edge computing. This reduces authentication delays, making the process nearly instantaneous. The entire system is optimized to consume minimal power, ensuring it does not significantly drain the bike's battery.

The Face Recognition Bike Starter offers a secure, contactless, and modern solution for bike ignition. By eliminating physical keys and digital passcodes, it enhances security, reduces theft risks, and provides a seamless experience for riders, making it an ideal upgrade for modern two-wheelers.



VII. SIMULATED OUTPUTS

To simulate the Face Recognition Bike Starter, we can use Python with OpenCV and a deep learning model to detect and recognize faces. The system will compare a live captured face with stored images and decide whether to start the bike or not. The simulation will include:

1. Capturing a live image from the webcam
2. Comparing it with stored face data
3. Authenticating the user
4. Simulating the bike start mechanism

Here's the Python code for the simulation:

```
import cv2
import numpy as np import
os
# Load the pre-trained face recognizer and Haar cascade for face detection

face_cascade = cv2.CascadeClassifier(cv2.data.haarcascades + 'haarcascade_frontalface_default.xml')
recognizer = cv2.face.LBPHFaceRecognizer_create()

# Load pre-trained model (Ensure 'trainer.yml' exists after training with authorized faces)
```

```
if os.path.exists("trainer.yml"):
    recognizer.read("trainer.yml")
else:
    print("Error: No trained model found. Train themodel first.") exit()

# Define user IDs (Modify based on stored user data)
authorized_users = {1: "Authorized User"}

# Open webcam
cap = cv2.VideoCapture(0)

while True:
    ret, frame = cap.read()
    gray =
    cv2.cvtColor(frame, cv2.COLOR_BGR2GRAY)  # Convert to grayscale

    # Detect faces in the frame
    faces = face_cascade.detectMultiScale(gray, scaleFactor=1.2, minNeighbors=5, minSize=(100, 100))

    for (x, y, w, h) in faces:
        face_id, confidence = recognizer.predict(gray[y:y+h, x:x+w])

        # If confidence is below a threshold, authentication is successful
        if confidence < 50:  # Lower value means better match
 user_name = authorized_users.get(face_id, "Unknown")
            cv2.putText(frame, f"Access Granted: {user_name}", (x, y-10), cv2.FONT_HERSHEY_SIMPLEX, 0.8, (0, 255,
0), 2)
            cv2.rectangle(frame, (x, y), (x+w, y+h), (0, 255, 0), 2)
            print("Face Recognized! Bike Started ")
        else:
            cv2.putText(frame, "Access Denied", (x, y-10), cv2.FONT_HERSHEY_SIMPLEX, 0.8,
(0, 0, 255), 2)
            cv2.rectangle(frame, (x, y), (x+w, y+h), (0, 0, 255), 2)
            print("Unauthorized Face! Bike Locked ")
    cv2.imshow('Face Recognition Bike Starter', frame)

    if cv2.waitKey(1) & 0xFF == ord('q'): break

cap.release() cv2.destroyAllWindows()
```

VIII .FUTURE ENHANCEMENTS

The Face Recognition Bike Starter system is an innovative approach to vehicle security, providing a keyless and hands-free ignition system. While the current implementation offers enhanced security and convenience, future advancements can further improve accuracy, reliability, and usability. Below are some key future enhancements that can be integrated into the system to make it more robust and efficient.

1. Multi-Factor Authentication (MFA)

To enhance security, a multi-factor authentication (MFA) system can be introduced. In addition to face recognition, other authentication methods such as fingerprint scanning, voice recognition, or mobile-based authentication can be integrated. This ensures that even if an unauthorized person tries to spoof the system using a high-quality image or video, the bike remains secure.

2. AI-Powered Anti-Spoofing Mechanisms

Currently, face recognition systems are vulnerable to spoofing attacks using printed images or videos.

To prevent unauthorized access, advanced AI-powered anti-spoofing mechanisms can be implemented. Techniques like liveness detection**,** which verifies facial movements (blinking, head tilting, or lip movement), can be used to distinguish real users from fraudulent attempts. Additionally, 3D depth-sensing cameras can be used to detect the depth and structure of a person's face, making it difficult to bypass the system.

3. Cloud-Based User Authentication

Integrating cloud-based authentication can allow users to store their facial data securely on a remote server. This would enable users to access their bike from multiple devices and provide an added layer of security. In case a user loses their bike or needs to

update their credentials, they can manage their profile remotely without needing direct access to the bike's hardware.

Mobile App Integration

A dedicated mobile application can be developed to provide users with greater control over the bike's security system. Through the app, users can:

- Remotely authorize access to family members or friends.
- Receive security alerts in case of unauthorized access attempts.
- Track real-time GPS location of their bike to prevent theft.
- Enable emergency access through a secure PIN or backup authentication.

4. Voice Command Ignition

To enhance user convenience, voice command ignition can be added as an alternative to facial recognition. AI-powered voice recognition can allow users to start the bike using predefined voice commands. This feature would be particularly useful in cases where the camera system fails due to poor lighting or other environmental conditions.

5. Integration with IoT and Smart Locks

Integrating Internet of Things (IoT) technology can improve the system's functionality. A smart lock system controlled via facial recognition and a mobile app can enhance security. Users can remotely lock or unlock their bike, and the system can automatically disable ignition in case of suspicious activity.

6. Real-Time Environmental Adaptation

The current system may struggle in extreme lighting conditions (too bright or too dark). Future versions can include adaptive illumination using infrared cameras or dynamic brightness adjustments to improve recognition accuracy. This will ensure seamless operation under all lighting conditions, including nighttime.

7. Automatic Helmet Detection

For rider safety, an automatic helmet detection system can be added. The bike will only start if the user is recognized and wearing a helmet. This feature can be implemented using object detection techniques in computer vision.

8. Faster Processing with Edge AI

Currently, face recognition processing happens on a local microcontroller (such as Raspberry Pi or Arduino). Future enhancements can utilize Edge AI technology, which processes facial recognition data on-device rather than relying on cloud-based servers. This will significantly reduce processing time and improve real-time performance.

9. Emergency SOS Feature

In case of accidents or emergencies, an SOS feature can be added to the system. If the bike detects a crash or an impact, it can automatically send an alert with the rider's location to emergency contacts or authorities. This can be done using IoT- based sensors and mobile connectivity.

IX. CONCLUSION

The Face Recognition Bike Starter is an innovative security solution that replaces traditional key- based ignition with facial recognition technology. This system ensures that only authorized users can start the bike, significantly reducing the risk of theft and unauthorized access. By integrating real- time image processing, deep learning-based authentication, and microcontroller-controlled ignition, the system offers a seamless and secure experience. Unlike physical keys, which can be lost or duplicated, facial recognition provides a more reliable and efficient alternative.

The system captures the rider's face using a high-resolution camera, processes the image using AI algorithms, and compares it with stored facial data for authentication. If a match is found, the bike starts automatically; otherwise, access is denied. Future improvements such as multi-factor authentication, AI-powered anti-spoofing, mobile app integration, and IoT-based security can further enhance its effectiveness. Real-time environmental adaptation and edge AI can also optimize performance under different conditions.

Overall, the Face Recognition Bike Starter modernizes bike security by offering a hands-free, keyless ignition system. With continuous advancements, it has the potential to become a standard feature in future two-wheelers, providing enhanced security, convenience, and a futuristic riding experience.

REFERENCES

1. A. George, C. Ecabert, H. O. Shahreza, K. Kotwal and S. Marcel, "EdgeFace: Efficient Face Recognition Model for Edge Devices," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 6, no. 2, pp. 158-168, April

2024, doi: 10.1109/TBIOM.2024.3352164.

2. Zhang, "Detect Faces Efficiently: A Survey and Evaluations," in IEEE Transactions on Biometrics, Behavior, and Identity Science, vol. 4, no. 1, pp. 1-18, Jan. 2022, doi:10.1109/TBIOM.2021.3120412.

3. P. C. Neto, J. R. Pinto, F. Boutros, N. Damer, A. F. Sequeira and J. S. Cardoso, "Beyond Masks: On the Generalization of Masked Face Recognition Models to Occluded Face Recognition," in *IEEE Access*, vol. 10, pp. 86222- 86233, 2022, doi: 10.1109/ACCESS.2022.3199014.

4. J. G. Cavazos, P. J. Phillips, C. D. Castillo and A. J. O'Toole, "Accuracy Comparison Across Face Recognition Algorithms: Where Are We on Measuring Race Bias?," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 3, no. 1, pp. 101-111, Jan. 2021, doi: 10.1109/TBIOM.2020.3027269.

5. P. Terhörst, M. Huber, N. Damer, F. Kirchbuchner, K. Raja and A. Kuijper, "Pixel-Level Face Image Quality Assessment for Explainable Face Recognition," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 5, no. 2, pp. 288-297, April 2023, doi: 10.1109/TBIOM.2023.3263186.

6. Z. Zhu *et al*., "WebFace260M: A Benchmark for Million-Scale Deep Face Recognition," in *IEEE Transactions on Pattern Analysis and Machine Intelligence*, vol. 45, no. 2, pp. 2627-2644, 1 Feb. 2023, doi: 10.1109/TPAMI.2022.3169734.

7. Z. Yang, J. Liang, C. Fu, M. Luo and X. -Y. Zhang, "Heterogeneous Face Recognition via Face Synthesis With Identity-Attribute Disentanglement," in *IEEE Transactions on Information Forensics and Security*, vol. 17, pp1344-1358, 2022.

8. S. Malakar, W. Chiracharit and K. Chamnongthai, "Masked Face Recognition With Generated Occluded Part Using Image Augmentation and CNN Maintaining Face Identity," in *IEEE Access*, vol. 12, pp. 126356-126375, 2024, doi: 10.1109/ACCESS.2024.3446652.

9. H. Otroshi Shahreza and S. Marcel, "Template Inversion Attack Using Synthetic Face Images Against Real Face Recognition Systems," in *IEEE Transactions on Biometrics, Behavior, and Identity Science*, vol. 6, no. 3, pp. 374-384, July 2024, doi: 10.1109/TBIOM.2024.3391759.

10. W. Hu, W. Yan and H. Hu, "Dual Face Alignment Learning Network for NIR-VIS Face Recognition," in *IEEE Transactions on Circuits and Systems for Video Technology*, vol. 32, no. 4, pp. 2411-2424, April 2022, doi: 10.1109/TCSVT.2021.3081514.