Research Square

Preprints are preliminary reports that have not undergone peer review.
They should not be considered conclusive, used to inform clinical practice,
or referenced by the media as validated information.

Design and Implementation of an Embedded System for Vehicle Anti-Theft Using Face Recognition and Live Location Tracking on Raspberry Pi

Ayman Elshenawy
Al-Ahliyya Amman University
Khalil M. Abdelnaby
k.abdelnaby@ammanu.edu.jo
Al-Ahliyya Amman University
Mohamed A. Rohaim
Al-Ahliyya Amman University
Ayman Mohamed
Al-Ahliyya Amman University
Ahmad Shalaldeh
Al-Ahliyya Amman University
Malik AL-Essa
University of Jordan

Research Article

Keywords: Vehicle Security, Intelligent Vehicle Anti-Theft System, Mobile Control & Tracking Keyless Entry, Embedded Systems, Raspberry Pi, ATmega32, IoT, VGG16

Posted Date: March 16th, 2026

DOI: https://doi.org/10.21203/rs.3.rs-8964937/v1

License: This work is licensed under a Creative Commons Attribution 4.0 International License.
Read Full License

Additional Declarations: No competing interests reported.

Design and Implementation of an Embedded System for Vehicle Anti-Theft Using Face Recognition and Live Location Tracking on Raspberry Pi

Ayman Elshenawy[1], Khalil M. Abdelnaby[1,2,*], Mohamed A. Rohaim[1,2], Ayman Mohamed[1], Ahmad Shalaldeh[1], Malik AL-Essa[3],

[1]Faculty of Information Technology, Al-Ahliyya Amman University, Amman 19111, Jordan.
[3]Systems and Computers Engineering Department, Faculty of Engineering, Al-Azhar University, Nasr City 11765, Cairo, Egypt.
[3]Computer Science Department, The University of Jordan, Jordan.
Corresponding Author: Khalil M. Abdelnaby (e-mail: k.abdelnaby@ammanu.edu.jo)

Abstract: The rapid advancement of Information Technology, which has driven down vehicle prices, has led to a substantial increase in global vehicle sales over the past two decades. However, this rise in vehicle ownership has also been accompanied by a notable surge in car theft, creating a significant challenge for vehicle owners. As a result, a continuous battle exists between vehicle manufacturers and thieves. Unfortunately, traditional security methods often fall short when facing increasingly sophisticated vehicle theft techniques, which leads to the vehicle theft problem becoming a global issue. This paper proposes an Intelligent Vehicle Anti-Theft System (IVATS) as a solution for the vehicle theft problem. The proposed IVATS integrates GSM, GPS, Raspberry Pi, and a novel Challenge-Response Face Authentication model to improve the system security. The IVATS addresses limitations of existing solutions, such as reactive responses, unreliable user verification, and poor scalability, by integrating real-time tracking, remote mobile control, and multi-layered biometric authentication. The research contribution is threefold: (1) a high security framework leveraging IoT and embedded systems, (2) a challenge-response face authentication model incorporating emotion verification to deter spoofing, and (3) a user-friendly mobile app for remote monitoring. The IVATS employs a Raspberry Pi 3 and ATmega32 microcontroller to manage hardware modules (camera, GPS, GSM) and software components, including a Horizontal Ensemble Best N-Losses (HEBNL) model, which is a fine-tuned VGG16 model for emotion recognition. The challenge-response face authentication model achieves an average accuracy of 98.89% under optimal lighting but may degrade in low-light conditions and can authenticate users in 24 ms, which is suitable for the hardware devices that constitute the system. The integration of CRFA with FER outperforms traditional VATS by enabling dynamic, liveness-aware authentication based on real-time emotional responses, which substantially mitigates spoofing and replay attacks while preserving low-latency performance on embedded platforms. Moreover, IVATS offers a practical and efficient solution for modern vehicle security by effectively balancing strong robustness with user convenience.

Keywords: Vehicle Security, Intelligent Vehicle Anti-Theft System, Mobile Control & Tracking Keyless Entry, Embedded Systems, Raspberry Pi, ATmega32, IoT, VGG16.

I. Introduction

Vehicle theft is one of the most widespread and continuously growing crimes in the world, placing vehicle owners in a very risky position and continuously subjecting them to great threats and economic losses. Manual protective measures, such as mechanical locks and alarm systems, are no longer effective against car thieves who have the skills to bypass these security devices using advanced techniques [1]. Furthermore, traditional anti-theft techniques cannot always stand against the advanced thinking of the thieves [2]. This always indicates an urgent need for a much-improved and integrated security system. Therefore, there is an increasing demand for innovative and updated Vehicle Anti-Theft Systems (VATS) capable of countering these evolving theft techniques [2].

There is a growing demand for innovative and intelligent Vehicle Anti-Theft Systems (VATS) that can counter evolving theft methods effectively. The Internet of Things (IoT) has emerged as a powerful tool in this domain, offering solutions across various areas, including IoT-enabled network models [3], autonomous vehicles [4], and smart agriculture [5]. Specifically, IoT technologies have shown great promise in enhancing vehicle security through smart sensor networks and real-time communication systems [1, 6]. Recently, researchers have been involved in finding various ways through which vehicle security could be enhanced against theft. Some of these studies have been specifically made to integrate the recent technologies into VATSs to increase their efficiency.

VATS consists of [7]: (i) a Global Positioning System (GPS) module used for live tracking by determining the vehicle's location using satellite signals. (ii) Global System for Mobile

Communications (GSM) module, which is used to facilitate communication between the vehicle controller and the user's mobile device or email by sending the vehicle location data and behavioral alerts via cellular networks. (iii) Microcontroller unit, which represents the system's brain that processes its input and publishes its responses, like sending messages, alarms, and activating proactive procedures such as immobilization. (iv) other supportive systems such as alarm systems, and a power [8, 9, 10]. Global VATS systems usually integrate two main functional subsystems: the security subsystem, which is used to detect unauthorized users, verify authorized users, and activate alerts, shocks, or immobilization for theft prevention, and the real-time tracking subsystems that are used for vehicle tracking and vehicle theft recovery [11-14].

Although some of the existing systems may have some features, either GPS tracking or remote immobilization, the rest lack the sophistication and integration that would help to give appropriate protection against theft or unauthorized access. In addition, the lack of reliable methods for owner authentication makes a vehicle prone to unauthorized use, compromising its safety features [2, 1].

A. VATS Security Sub-System

VATS's security subsystem is developed using various technologies, whereas (i) Some VATS are designed based on RFID authentication [12] to link the mobility of the vehicle to the presence of its owner [12]. Another class works by applying a dual security system using both a password input and vehicle owner notification by sending a one-time password (OTP) using GSM technology [15]. In addition, there are also VATSs that introduce a driver identity verification using iris recognition [16]. The techniques and systems mentioned perform well, but still, some limitations exist based on the utilized VATS technology, e.g., fingerprint scanning can be unreliable if the user's thumb is oily or dirty [12]. Password-based VATS has the potential for simple passwords and can be vulnerable to digital attacks [17].

Face recognition is a biometric technology that has gained increasing attention over the past few decades. It utilizes modern computer programs to recognize and verify a person's identity. It developed through several stages, starting with analyzing facial geometric features and ending with advanced deep learning [18, 19]. Face recognition is embedded in the VATS security subsystem as an enhancement to vehicle owner verification and authentication [20, 21]. Some VATSs utilize facial recognition applications to identify the vehicle owner or other authorized users through advanced computer vision-based algorithms and provide an additional layer of security against unauthorized vehicle access [22]. Recently, researchers have used face recognition as a main component of VATS security to improve the security of VATS systems [23-29] by integrating various techniques together. However, VATS with face recognition still suffers from limitations such as: (i) It can degrade under poor lighting, occlusions, dynamic environments, or variations in facial expressions [23]. (ii) It is vulnerable in areas with poor network coverage and spoofing with photos or videos [26, 25]. These limitations have prompted researchers to consider alternative techniques that may offer improvements.

B. VATS Real-time Tracking Sub-System

Real-time Tracking Sub-system in VATS is used to provide the vehicle owner, in case of theft, with the current and historical location of the vehicle in real-time [30, 31]. One example is the real-time tracking framework proposed in [32]. It utilizes recent technologies such as GPS tracking, remote vehicle immobilization, and real-time monitoring features for efficient vehicle theft prevention and recovery. The framework proved that it is possible to integrate several technologies to get a strong, intellectual VATS. Another system integrates GPS, GSM, and IoT to offer a practical solution to mitigate vehicle theft [33]. Other systems make tracking based on GPS trackers using IoT, and authentication using both RFID tags and fingerprint scanners [34].

Real-time Tracking Sub-systems in VATSs are subjected to some limitations that affect their performance, such as: (i) GPS and GSM-based systems depend on signal availability and are vulnerable to signal blocking, and traditional vehicle tracking sub-systems' security systems can be compromised by blocking their signals [12]. (ii) These devices are susceptible to power fluctuations and environmental factors like ambient temperature, potentially causing transmission latency. To mitigate these issues, the authors used two Arduino kits to provide a more reliable design [35]. (iii) A limitation of the system is its reliance on the availability and strength of the GSM/GPRS network [36]. (iv) Additionally, the cost and maintenance of the system components, as well as the scalability and long-term sustainability of the solution, are factors that require further consideration [33].

The abovementioned limitations are considered as motivation for the development performed in this research. Facial Emotion Recognition (FER) is a technique that analyzes facial expressions to identify emotional states, and it has become a significant area of interest in computer vision, computer graphics, security, and human-computer interaction (HCI) [37, 38]. To overcome limitations in face recognition in VATS's security, such as vulnerability to spoofing, liveness, and sensitivity to lighting and pose variations, FER offers a powerful solution by deeply understanding a person's emotional state [39, 40]. This integration not only enhances the accuracy and robustness of face recognition, especially in dynamic environments, thereby enhancing security, but also allows systems to adapt to emotional changes in facial appearance, ensuring more reliable identification across different expressions [41-42].

This paper presents an Intelligent Vehicle Anti-Theft System (IVATS) for comprehensive and robust vehicle security

against unauthorized access and theft, tracking, and adequate communication. The proposed IVATS utilizes the following technologies: (i) GSM technology included in vehicles to provide adequate communication with vehicle owners. (ii) GPS capability for vehicle tracking to provide an excellent chance of recovering the vehicle in case of theft. (iii) A Challenge-Response Face Authentication (CRFA) for owners' verification based on their face identities, in addition to some randomly identified emotion verification. (iv) mobile application to provide the user with a friendly interface form to interact with the vehicle remotely. The proposed IVATS achieves an average CRFA accuracy of 98.89% under optimal lighting conditions, with a False Acceptance Rate (FAR) as low as 0.13% for happy emotions and 1.5% for angry emotions, while the False Rejection Rate (FRR) ranges from 0.3% to 2.2%. The system's CRFA module processes emotions in just 24 ms per prediction, leveraging a fine-tuned VGG16 model enhanced by the Horizontal Ensemble Best N-Losses (HEBNL) technique, which achieves an average accuracy of 98.89% for the more expressive emotions, such as Happy, Surprise, Normal, and Angry emotions, ensuring high reliability in real-time vehicle security applications. The system's power consumption peaks at 7.5W during active authentication, balancing efficiency with computational demands on the Raspberry Pi 3 B+ hardware.

The contribution of this research paper can be summarized as follows:

i. A secure framework for effectual deterrence of unauthorized access to vehicles is designed using advanced technologies.
ii. A CRFA module is developed based on combining both face recognition and emotion verification for vehicle owner authorization and verification.
iii. The whole system is equipped with real-time monitoring and tracking to provide the vehicle's owner with real-time alerts in case of any suspicious activity or security breach. iv. A user-friendly remote control through mobile applications for ease of interaction with the IVATSs.

The paper is organized as follows: Section II discusses related work on VATSs. Section III presented the proposed IVATS. The IVATS main processes are presented in section IV. Section V provides system hardware and software implementation. Comparative study and performance Analysis are presented in section VI. Lastly, Section VII concludes the paper by summarizing the research, highlighting the contributions of IVATS, and suggesting future directions.

II. Related Work

Several studies have addressed the challenges of ATSs and proposed innovative solutions to mitigate the risk of theft and unauthorized access. This section provides an overview of relevant research and highlights recent advancements in the field. The systems designed to tackle this issue can be categorized into the following main categories:

A. Vehicle Tracking System

Pillai et al. discuss an ATS for two-wheeler vehicles. The system features include live location tracking, theft attempt notification, and user authentication through an Android application [43]. Chakole *et al.* introduced a cost-effective portable system for online and offline vehicle tracking and monitoring, employing Micro-Electromechanical System MEMS accelerometers and ultrasonic sensors for an antitheft system [44]. Shruthi *et al.* [45] proposed a Vehicle Tracking System (VTS) that combines in-vehicle microcontrollers, GPS, GSM, a web camera, and a user unit with a smartphone. The user can request the vehicle location, receive SMS alerts when the vehicle is moved, and capture images of unauthorized drivers. Taha *et al.* [46] introduced a VATS that utilizes an Arduino controller and SIM800L modules integrated with a GSM modem and GPS receiver to accurately determine the vehicle's location. Data is transmitted to a remote server through TCP, enabling visualization on web maps. Zhiwei *et al.* [47] investigated brake-induced stick-slip vibrations in vehicle-track systems, emphasizing the critical role of nonlinear disc-pad friction. Their dynamic model uncovers how these nonlinearities compromise braking stability, offering actionable design principles to mitigate vibration risks in rail and automotive systems. Guojun *et al.* [48] developed a spatial dynamics model for rack vehicle-track systems, explicitly integrating multi-stage gear transmission effects. Their work demonstrates that time-varying mesh stiffness and dynamic excitations significantly alter wheelset vibrations, with field-validated results underscoring the model's utility for stability optimization. Guofang *et al.* [49] analyzed vehicle-track dynamics in seasonal frozen transition zones, quantifying how combined mechanical and thermal excitations degrade system performance. This study provides climate-specific design guidelines to enhance the durability and safety of rail infrastructure in vulnerable regions.

B. Vehicle Security System

Rachit *et al.* [50] presented an embedded Vehicle Security System (VSS) device designed to enhance vehicle security based on IoT to provide features such as an alert system, live tracking, Wi-Fi connectivity, and dashboard camera monitoring. Prakash et al. presented a VTS [51] that utilizes GSM, GPS, a vibration sensor, and a MEMS sensor to detect unauthorized vehicle use, notify the owner via SMS, and activate a buzzer. In addition, the remote control of the engine is used to turn off the vehicle.

Roupesh *et al.* [52] introduced a robust VSS using RFID technology to prevent the theft of coal trucks in mines. The system verifies the vehicle's original number with the number plate using an RFID module, allowing authorized vehicles to enter while alerting the authorities in case of a

mismatch. Islam *et al.* [53] presented a two-step VSS for theft prevention and real-time tracking of cargo vehicles using IoT. The system addresses the problem of car theft during transportation, which disrupts the supply chain and causes financial losses. The system has features such as locking and unlocking the outer door seal, real-time tracking of cargo status, and alert mechanisms in case of security breaches.

Viswanatha *et al.* [27] presented an AI-enabled smart vehicle security system that combines CNN and DeepFace for anti-theft detection. Using Haar-Cascade for real-time face detection and DeepFace for identity verification, the system prevents unauthorized access by triggering SMTP-based email alerts with intruder images. The system is implemented on a Raspberry Pi 4B, achieving an accuracy of 97.41% accuracy, 100% precision, and 98.69% F1-score, outperforming existing methods. The system offers a robust, real-time solution for vehicle theft by leveraging IoT and deep learning for improved security.

Renjith *et al.* [54] introduced an innovative risk assessment framework for autonomous vehicles that combines LSTM networks with real-time sensor fusion and V2V communication. Their trust evaluation model shows notable improvements in both threat detection accuracy and response latency, marking a significant step toward safer autonomous operations. Izhar *et al.* [55] developed a zero-trust security model specifically designed for IoT-connected autonomous vehicles. Their context-aware system implements dynamic access controls and continuous behavioral monitoring, creating an adaptive defense mechanism against evolving cyber threats in vehicular networks.

Richard *et al.* [56] provided a comprehensive examination of cybersecurity challenges in connected vehicles, analyzing how increased system complexity creates new attack surfaces. Their work highlights critical privacy concerns and proposes mitigation strategies, underscoring the urgent need for more resilient security frameworks in modern automotive design.

C. Vehicle Biometric Authentication System (VBAS)

Mahesh *et al.* [57] proposed an embedded VBAS system to enhance vehicle security and driver monitoring. The system utilizes a high-resolution camera, Raspberry Pi, vibration sensor, and open-source software to allow access to the vehicle by comparing the person's image with the authorized individuals, capturing images in case of denial, and sending them to the owner.

Raj *et al.* [58] introduced a VBAS using fingerprint recognition for securing Electric Vehicles (EVs). The system prevents unauthorized access and vehicle theft by incorporating fingerprint scanning. Microcontrollers are used to store and verify authorized fingerprints, ensuring only authorized individuals can access the vehicle's lock. Srinivasarao *et al.* [59] combined wireless fingerprinting, Arduino, RFID reader, and GSM technology to provide cost-effective VBAS for theft protection in vehicles. Using driver's licenses and authenticated fingerprints, the system allows authorized individuals to operate the vehicle while deterring unlicensed drivers to enhance vehicle security.

Singh *et al.* [60] introduced a VBAS based on facial recognition technology using Raspberry Pi to detect unauthorized access and identify individuals through facial recognition. Srinivas *et al.* [61] presented a fingerprint VBAS for an anti-theft detection and alerting system designed to enhance vehicle security. They provide robust authentication and access control by incorporating multi-layered security measures such as engine immobilization and alarms to deter unauthorized access.

Jeevitha *et al.* [62] introduced a VBAS for theft identification and prevention using GPS location tracking. The system utilizes fingerprint recognition to secure vehicles against unauthorized entry. It integrates GPS and GSM-based anti-theft car monitoring systems to track the vehicle's location in real time and aid in the recovery of stolen vehicles. Teradal *et al.* [63] introduced a comprehensive IoT-based security system that combines license plate recognition with fingerprint authentication to create a multi-layered theft prevention solution. Their prototype demonstrates how real-time image processing and biometric verification can significantly enhance vehicle security compared to conventional key-based systems.

Shin *et al.* [64] developed a novel framework that utilizes CAN bus data processed through an MLOps platform. By implementing sophisticated feature extraction and ensemble learning techniques, their system achieves highly accurate driver recognition, enabling both enhanced security measures and personalized vehicle settings. Wang *et al.* [65] proposed a blockchain-based authentication mechanism specifically designed for UAV-assisted networks. Their innovative approach employs smart contracts and advanced cryptography to establish a decentralized, tamperproof identity verification system that effectively mitigates common attack vectors like spoofing while maintaining operational efficiency in dynamic environments.

D. Vehicle Anti-Theft Systems (VATS)

Dey *et al.* [66] presented an embedded VATS system for preventing vehicle theft using GSM, GPS, and fingerprint verification. GSM and GPS technology are used to track the vehicle's location in real time. Fingerprint verification ensures that only authorized individuals can drive the vehicle. Singh *et al.* [67] introduced a Bluetooth-enabled VATS using an Android-based handheld device. The system utilizes biometric authentication, specifically fingerprint recognition, to provide a foolproof mechanism against vehicle theft. The proposed solution can be deployed in various types of vehicles and allows access only to intended users.

Noman *et al.* [14] developed a VATS that utilizes a microcontroller, GPS-GSM modules, RFID, and a tilt sensor

to enhance vehicle security. It allows for authentication through RFID, fingerprint, or password, sends the vehicle's location to the owner via GPS, GSM, and incorporates an alarm and fuel injector deactivation to prevent unauthorized use. Qian *et al.* [68] developed an Android VATS based on the Android operating system in a hand-held communication terminal. By utilizing the built-in sensors of the terminal, abnormal vehicle information is sent through the communication network, enabling long-distance remote alarm and tracking. Lappanitchayakul *et al.* [69] proposed a VATS that uses radio wave technology and LoRa transmission to instantly detect car movement and send the GPS location to the owner. Palacean *et al.* [70] introduced an optimized architecture for IoT-enabled GPS ATS for EVs.

Balakrishnan *et al.* [24] proposed a VATS that incorporates face recognition using Raspberry Pi and IoT technology to address the limitations of existing systems by using face detection for identity verification. Vinay Kumar *et al.* [71] proposed a VATS system that protects EVs from theft. This system leverages sensor network technology along with GPS and GSM for tracking and incorporates features for an ATS. Thamoethata *et al.* [72] analyzed the existing VATS to address its limitations. The authors highlight the need for a VATS that is not embedded in the vehicle itself to effectively reduce vehicle theft rates.

Zhang *et al.* [73] pioneered an ARM-based embedded solution for electricity theft detection, employing real-time computational modeling to achieve unprecedented accuracy while maintaining energy efficiency. This innovative approach presents a scalable, cost-effective alternative for smart grid monitoring that could revolutionize power distribution security. Yijun *et al.* [74] developed an intuitive facial recognition system that translates user expressions into vehicle commands. Their computer vision framework, combined with adaptive control algorithms, demonstrates remarkable reliability in real-world testing while prioritizing safety. Vandabona *et al.* [75] conducted a comprehensive analysis of emergency vehicle sensor networks, exposing critical cybersecurity vulnerabilities while proposing a robust multilayered defense strategy. Their framework, validated through ambulance network case studies, effectively balances collision avoidance capabilities with protection against sophisticated attacks like jamming and spoofing.

E. Existing VATS Analysis

Despite the valuable contributions of existing research in the field of VATS, several limitations remain in the current systems, as follows:

- Most of the systems concentrate mainly on vehicle tracking and monitoring, giving less attention to theft cases.
- The user verification biometrics offer robust security; their exclusive use can lead to vehicle inaccessibility in scenarios like dirt or injury. Also, it may be attacked using a vulnerability.
- Most systems miss the integration with mobile applications, which makes these systems less usable and interactive than can be achieved using mobile apps.
- The dependence on SMS in some systems introduces challenges such as latency and limited bandwidth.
- Most of these systems are reactive, which only respond after a theft has already occurred. All these limitations highlight the need for a robust and proactive VATS to ensure vehicle security.

In this paper, a proactive Intelligent Vehicle Anti-Theft System (IVATS) is developed by integrating multiple technologies such as Challenge-Response Face Authentication (CRFA) for user verification, GSM for internet connection, and a mobile application for system usability and interactivity.

III. The Proposed IVATS

The proposed IVATS aims to provide an intelligent vehicle anti-theft system that addresses the limitations of traditional security measures. As shown in **Fig. 1**, the system is composed of the following main components:

A. CRFA Module

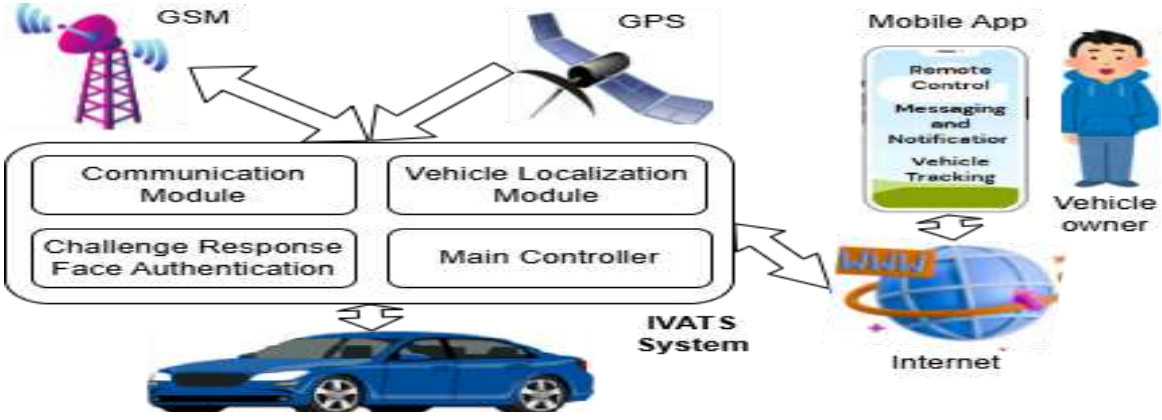


Fig. 1. Architecture of IVATS

The CRFA module is responsible for capturing the face of any user trying to access the vehicle. The user can access the vehicle only if the captured face is matched with the car owner's face saved in the system database. In addition to the person's face recognition, the CRFA module requires the user to express their emotions in at most three random emotions as a challenge. If the users pass this challenge provided by the system, the doors of the car will automatically unlock; otherwise, they will stay locked. In case of a break-in or a forced entry to the vehicle, the system will instantly pick up on the breach and send out warning messages to the owner.

The CRFA module enhances security to address vulnerabilities in traditional face authentication methods, such as spoofing attacks, by making the authentication process dynamic and unpredictable in IVATS. It prompts vehicle users with a random sequence of emotions, ensuring each authentication attempt is unique, as it demands a specific emotional response for each trial. This dynamic, real-time emotion elicitation makes it difficult for attackers to use pre-recorded images or videos to bypass the system. Furthermore, the enhanced accuracy of the CRFA module reduces the likelihood of false acceptances from such spoofed materials.

The IVATs CRFA module is highly robust against environmental factors, achieving 98.89% accuracy using the HEBNL technique and focusing on four easily expressed emotions (Happy, Normal, Angry, and Surprise). This robustness is due to the fine-tuning of the VGG16 architecture for emotion recognition. VGG-16 can effectively extract discriminative facial features even under poor lighting or partial occlusions, which makes CRFA robust and reliable against various environmental conditions. These metrics were derived from extensive testing on the KDEF dataset, which includes diverse facial expressions and lighting scenarios.

B. Vehicle Localization

This module utilizes GPS technology for precise tracking. It continually monitors the vehicle's location in real-time, allowing for rapid recovery in cases of theft, unauthorized use, or just for vehicle localization.

C. Anti-Theft Main Controller

This module acts as the central system for IVATS. It integrates advanced algorithms and a variety of sensors to detect unauthorized access or unusual behavior. Upon identifying a potential threat, it can trigger immediate responses such as immobilizing the vehicle or alerting law enforcement. It also communicates with the facial recognition module for access control.

D. Seamless Communication

This module establishes seamless connectivity between various components. It ensures that different parts of the system can communicate effectively and facilitate information exchange regarding security incidents to enhance the overall responsiveness and effectiveness of the system. Using this app, the owner can check all warning messages, know the status of the vehicle, track the geographical position of a vehicle in real-time, control the vehicle remotely, such as locking or unlocking the vehicle doors, and send instant alert messages against any kind of forced entry or break-in attempt to the owner.

IV. The IVATS Main Processes

Fig. 2 shows the flowchart that represents the main processes of the proposed IVATS. At the start, the system is in the initialization state to ensure that all its major key components are up and ready to work. The system starts with the initialization state through powering up the Raspberry Pi, GPS, and GSM modules, followed by the central microcontroller peripherals. During GSM initialization, the system performs network registration, establishes a TCP connection, connects to the set message broker, and subscribes to predefined topics. All these enable an instance to pull data from the broker without any hitch. The synchronization process can be relatively long. This module will generally conclude a boot process in about 7 seconds. The initialization process of a GPS module typically takes over a minute, influenced by factors like weather and environment. The Raspberry Pi initialization process starts with the user's provision of part of their essential information, basically their name, mobile phone number, and password for the system. Furthermore, the images on the face will be captured and saved for face recognition purposes.
The connectors C1 and C2 in **Fig. 2** are used to maintain the readability and logical structure of the IVATS flowchart. C1 acts as a merge point that unifies door-status and system-initialization decisions into a single control path, ensuring smooth continuation of system monitoring without redundant flow lines. This connector preserves the continuity of system operation by redirecting the control flow toward monitoring and access-handling logic once the Raspberry Pi, GSM module, and peripherals have been initialized. C2 represents a feedback loop connector associated with the authentication and retry logic of the IVATS system. It is activated when face identification fails or when authentication attempts remain within the allowed limit. It directs the control flow back to the authentication decision path, enabling repeated challenge–response attempts while enforcing the maximum attempt threshold. Once the attempt limit is exceeded, the flow exits this loop toward alarm activation. Thus, C2 implements controlled repetition in the CRFA process, ensuring both usability and security by balancing retry allowance with intrusion detection.

The following points offer a comprehensive explanation of the system's core functionalities, highlighting how each

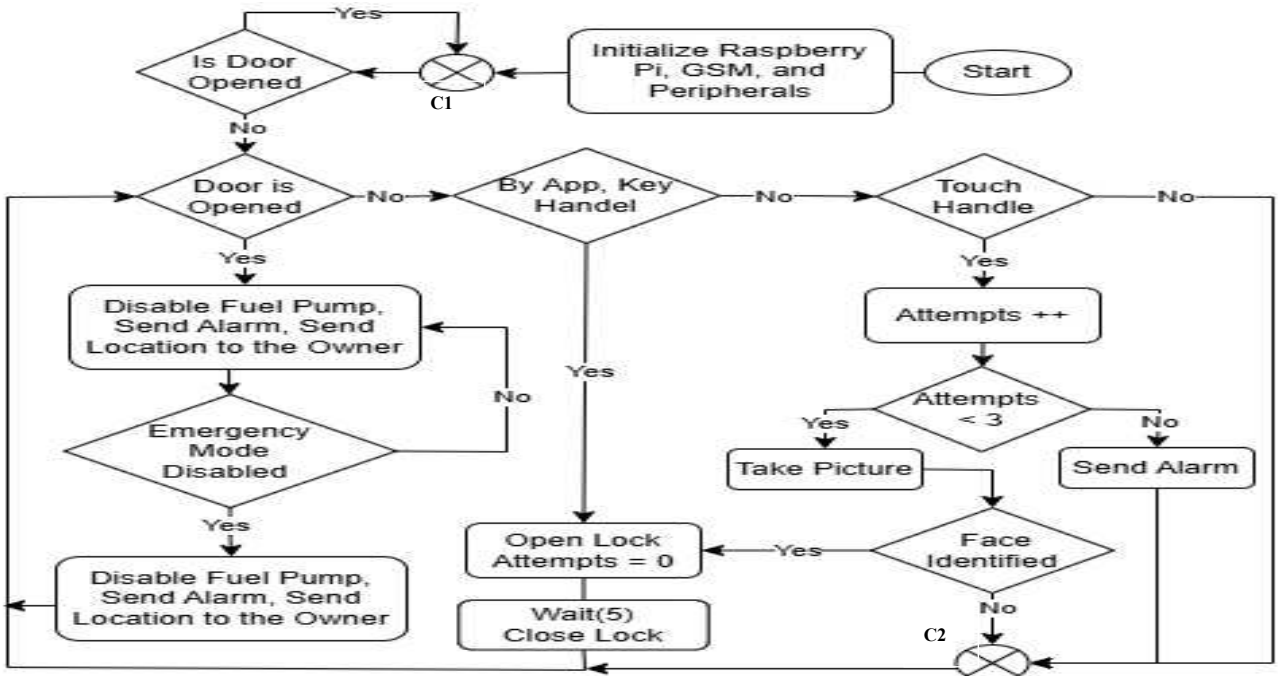


Fig. 2. IVATS Flowchart

component contributes to the overall operation and effectiveness of the system:

- **The operational state**: After the initialization process, the IVATS is now in operational mode, and, by default, the secured mode will automatically switch when the vehicle is turned on. Any unauthorized attempt at door opening transfers the system from the operational state to the emergency state.
- **The emergency state**: When the system enters an emergency state, it immediately disables the fuel pump, preventing unauthorized starting, even with the vehicle key. Simultaneously, it activates the vehicle's alarm to deter intruders and alerts nearby individuals. Additionally, the system broadcasts the vehicle's real-time location to the owner's mobile device, enabling them to track its whereabouts. The vehicle remains in this state until the owner sends an authenticated request to deactivate it. Upon successful authentication, the system deactivates the alarm, re-enables the fuel pump, and returns to standard operations once the doors are closed.
- **Remote Access and Automatic Locking**: During this state, the system is fully controlled through the mobile app. The system complies with remote unlock commands from the owner. However, the system automatically re-engages the locks if the door remains unopened for a specified period. Additionally, the owner can use the

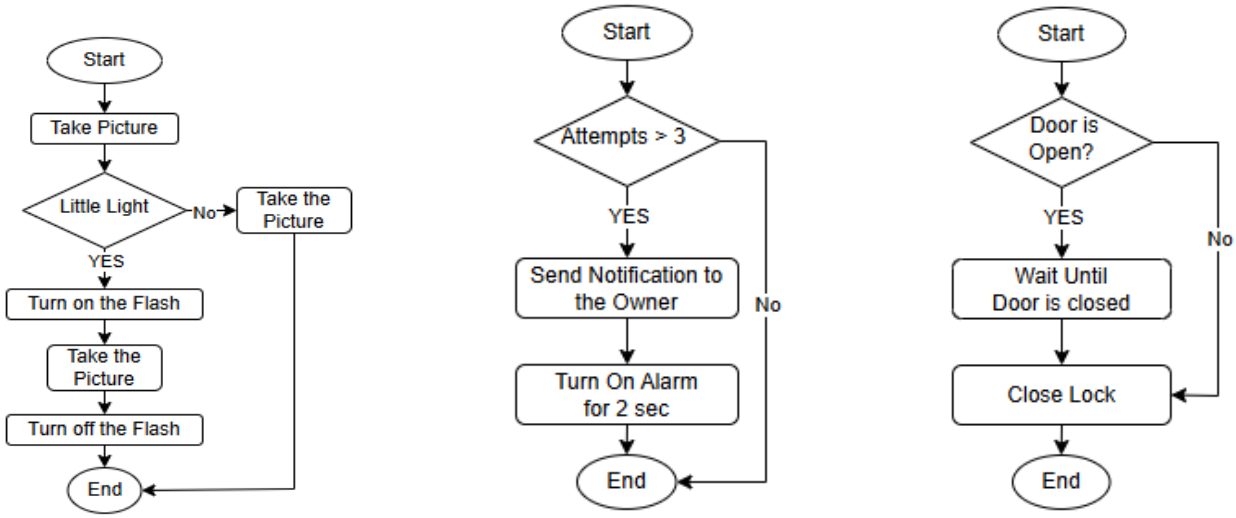


Fig. 3. (a) represents the flowchart of the take-picture process, (b) represents the flowchart of the send alarm process, and (c) represents the flowchart of the close lock process

manual key or the inner door handle to unlock and lock the vehicle.

- **Access Attempts and Facial Recognition:** During the operational state and interactions with the door handle, the IVATS system logs access attempts. If fewer than three attempts have been made and the ambient light is insufficient, the system briefly activates a flashlight to aid the camera in capturing a clear image. The computer vision module analyzes the image to determine if the individual is the vehicle owner. If recognized, the doors unlock. However, if the owner does not enter within a specific timeframe, the doors automatically re-lock. If the individual is not recognized, the vehicle remains securely locked. **Fig. 3** illustrates the flowcharts for taking pictures, sending alarms, and closing locks.
- Security Alerts and Alarm Activation: After three unsuccessful access attempts, the system sends a warning message to the owner's mobile device, indicating a potential security threat. If the number of attempts
- reaches or exceeds three, the vehicle's alarm activates for a two-second interval as an additional security measure.

V. System Implementation

A. Hardware Implementation

Fig. 4 illustrates the interconnected components of the IVATS and their interactions. The system is implemented using a Raspberry Pi 3 B+ and an ATmega32 microcontroller. The diagram highlights the connections of various modules, such as the camera, GSM, and GPS modules, as well as sensors and actuators, showcasing the system's versatility and potential applications in security and remote vehicle control. In this configuration, the Raspberry Pi serves as a centralized processing unit, efficiently managing tasks and establishing communication links with external networks. Simultaneously, the ATmega32 operates in real time, overseeing interactions with connected sensors and actuators. The Raspberry Pi 3 B+ is directly connected to the following hardware components:

- The camera module is designed to capture high-definition videos and photographs of individuals ranging from 165 cm to 190 cm in height, with a face length of approximately 25 cm. The camera is strategically positioned between the driver's door and the back door.
- GSM module: provides cellular communication capabilities encompassing data transfer, SMS, calls, and internet access.
- GPS module: delivers precise location tracking functionality.
- Touch display is connected via HDML to facilitate interaction through touch-based input. The ATmega32 microcontroller is directly connected to the following modules:
  - Flashlight: The microcontroller governs its activation or deactivation based on specific conditions.
  - Light Dependent Resistor (LDR): is employed for the measurement of light intensity.
  - Door sensor: is used for detecting the status of the vehicle door while it is open or closed.
  - Door handle sensor: a binary sensor designed to detect instances where a door handle is being utilized (e.g., touched), interacting via GPIO pins.
  - Buzzer: an audio signaling device capable of emitting sound alerts upon activation by the microcontroller.
  - Door lock: typically controlled via a motor through

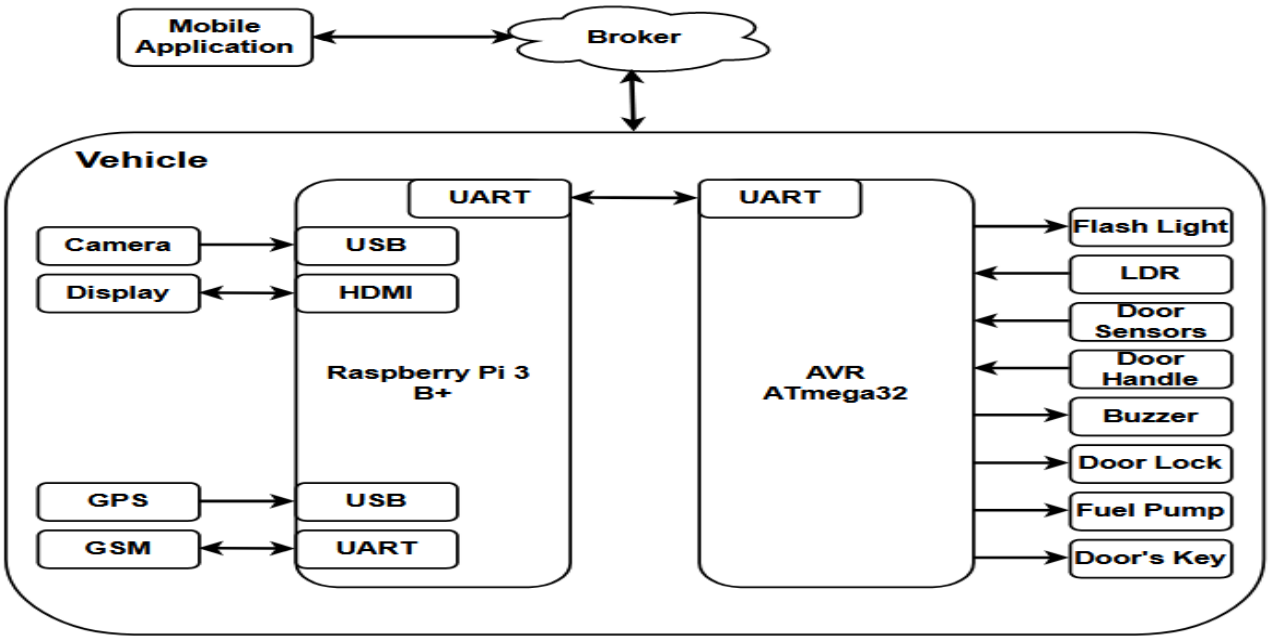


Fig. 4. IVATS architecture system implementation

- A relay circuit, enabling the microcontroller to lock or unlock a door.
- Fuel pump: The fuel pump's flow is regulated by the microcontroller.

The interconnection scheme for the proposed system's hardware components, including the AVR ATmega32 and Raspberry Pi, is depicted in Figs. 5 and 6, respectively.

B. Software Implementation

This section delves into the critical software components powering the IVATS, ensuring smooth, secure, and intelligent operations. The following is a list of the software tools utilized for implementing the system components and their main functions.

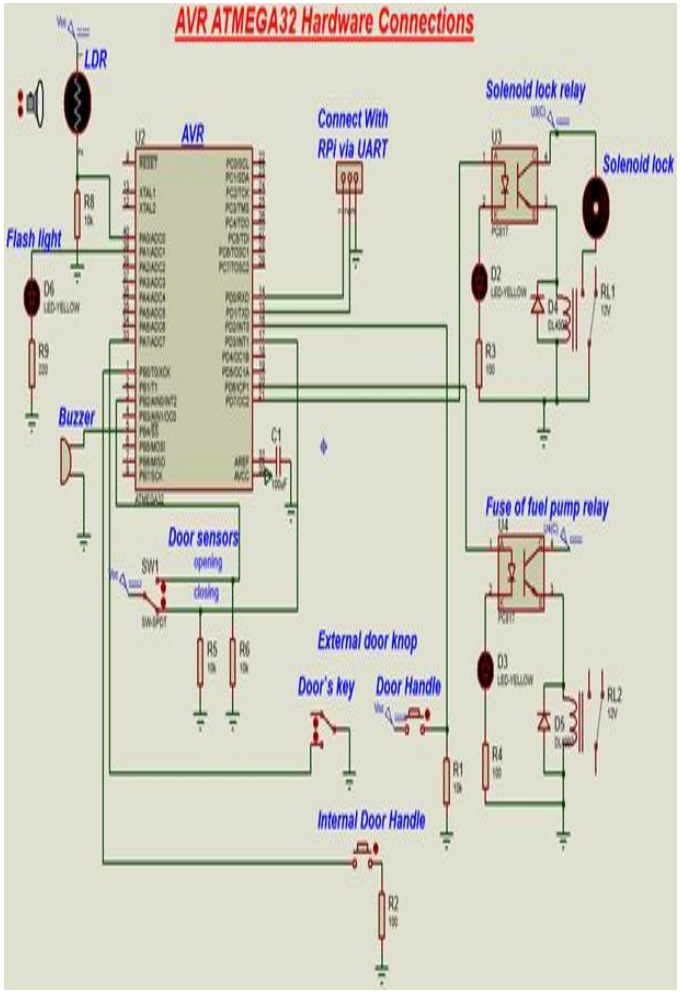


Fig. 5. AVR ATmega32 Hardware Connections

- **Communication protocol:** Communication protocols are a set of rules governing data exchange between network-connected devices. They establish rules and conventions for data transmission and reception. In IVATS, two types of communication protocols are utilized: (i) Wired Communication Protocols: Universal Asynchronous Receiver/Transmitter (UART) is used for serial communication with microcontrollers and peripherals, while SPI is used for high-speed data exchange with sensors and display modules. (ii) Wireless communication protocols: Wi-Fi is used for communication with Internet-connected devices, Bluetooth is used within personal area networks, and MQTT is used for lightweight and reliable messaging in IoT applications.

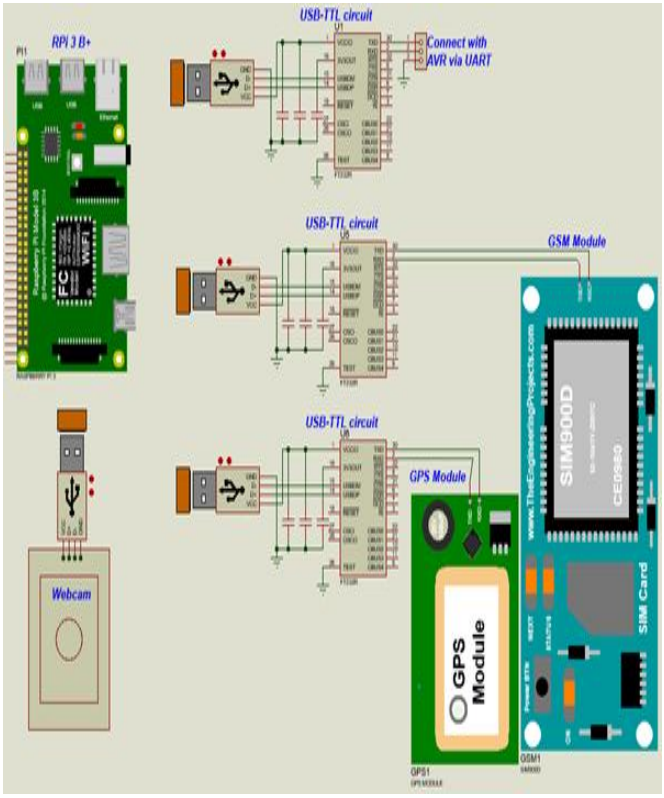


Fig. 6. Raspberry Pi Hardware Connections

- **Challenge-Response Face Authentication (CRFA):** The CRFA module consists of two main components: (i) a face authentication component that detects faces in the captured image for any person trying to access the vehicle, whether they are the vehicle owner or not. After that, it encodes the image and compares it with the owner's face image stored on the IVATS. **Fig. 7** illustrates the enhanced face authentication process, incorporating a challenge-response component [41]. (ii) Challenge Response emotion recognition: This sub-system employs emotion recognition as a challenge, requiring users to express three random emotions. The pre-trained VGG16 model is adapted and retrained to classify four specific emotions (happy, Surprise, normal, or Angry). The model is fine-tuned to optimize the number of layers and focus on easily displayable emotions. A HEBNL method combines predictions from these four models to improve performance.

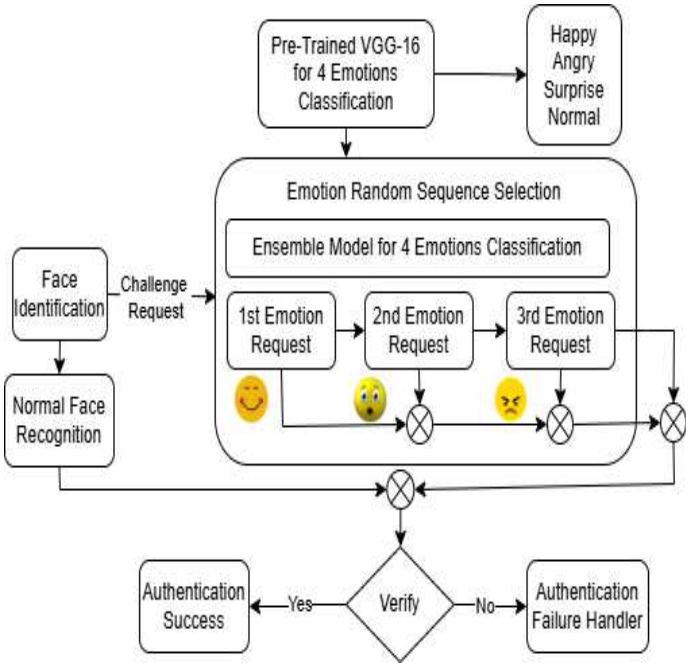


Fig. 7. Challenge-Response Face Authentication

The Karolinska Directed Emotional Faces (KDEF) [76] dataset is used for training and evaluating the proposed CRFA algorithm. The KDEF dataset is a widely recognized collection of facial expressions depicting seven basic emotions: happy, surprise, sad, disgust, angry, fear, and neutral. It consists of high-quality images of individuals from diverse demographics, captured under controlled lighting conditions, with each emotion displayed from multiple angles. In this study, we specifically focus on a subset of four emotions: happy, angry, surprise, and neutral, selected based on a user survey for their ease of expression and practicality in authentication scenarios. In the preprocessing phase, we employ the VGG16 model, a pre-trained Convolutional Neural Network (CNN) originally trained on the ImageNet dataset. The preprocessing steps involve replacing the top fully connected layer of VGG16 to adapt it for emotion classification, first with seven output classes (aligning with the KDEF emotions) and later refining it to four classes. The model is fine-tuned by retraining specific layers, starting from the last layer and moving backward to identify the optimal retraining point (layer index 15, "Block5_Conv1"), which achieved the highest accuracy. Additionally, we apply a horizontal ensemble technique to improve robustness by combining predictions from multiple models generated during training. The dataset is evaluated using 10-fold cross-validation, ensuring stratified sampling to maintain emotion distribution across folds. This preprocessing pipeline enhances the model's ability to generalize and achieve high accuracy (98.89%) in emotion recognition for authentication purposes. The system can operate in dual mode, with a configuration parameter (Disable_Challenge_Response) allowing for normal mode operation. Upon successful authentication, IVATS grants access based on the recognized identity. During authentication, the system randomly selects up to three emotion challenges from four predefined emotions (Happy, Normal, Angry, and Surprise), with the sequence varying each session to ensure unpredictability. The user must express each prompted emotion within a set time window, and facial images are processed in real time using a fine-tuned VGG16 model enhanced with the HEBNL technique. Access is granted only if the recognized emotions match the challenges within the allowed attempts; otherwise, the system triggers an alert or emergency state. This randomized, multi-step challenge–response mechanism provides inherent liveness verification and improves resistance to spoofing and replay attacks compared to static face recognition approaches.

- **IVATS Mobile App**: The IVATS mobile app empowers vehicle owners to remotely manage car security features. User registration allows vehicle owners to input personal data like name, mobile number, password, and facial recognition settings. Vehicle security features enable remote control of door locks, emergency mode activation, monitoring, and logout. The user-friendly interface allows vehicle owners to connect their cars to the app and configure settings. Additionally, the app provides real-time vehicle location tracking using a visual road map. The mobile app is developed using Java with Android Studio, the user interface is designed using Figma, backend integration is implemented using Android REST API calls, and location tracking is powered by Google Maps API. The mobile app interface offers a visually appealing and user-friendly way for vehicle owners to interact with their car security system. **Fig. 8** describes the mobile app of the workflow, and **Fig. 9** shows two screenshots of the IVATS mobile app interface, representing the home page of the mobile app and tracking the car location features.

VI. Comparative Study and Performance Analysis

We conclude this discussion by analyzing the performance of IVATS and comparing it to that of several related methods, selected from the recent state of the art. The HEBNL selects the top-performing models during training to achieve accuracy for happy emotion, surprise emotion, normal emotion, and angry emotion, respectively. The confusion matrix in **Fig. 10** reveals a strong overall performance with a high percentage in a truly positive rate. Furthermore, the misclassification rates for these emotions are minimal. This demonstrates that the model is highly accurate in distinguishing happy, surprise, normal, and angry emotion states. **Table 1** shows Accuracy, True Positive (TP),

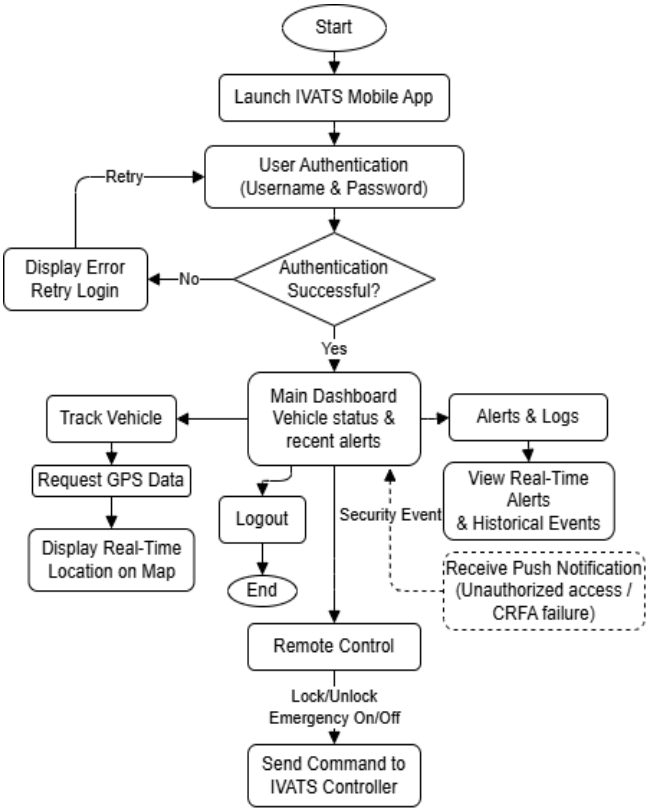


Fig. 8. The mobile app workflow.



(a) Home Page (b) track activity

Fig 9. Track the dynamic location feature of the IVATS mobile App.

Misclassification rate, False Acceptance Rate (FAR), and False Rejection Rate (FRR). The inference performance of the proposed CRFA module is evaluated directly on Raspberry

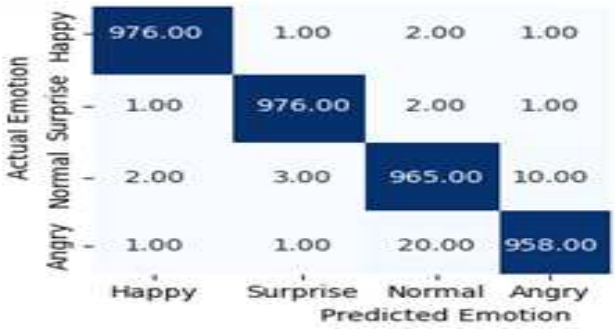


Fig 10. CRFA confusion matrix.

Pi 3 Model B+, to ensure that the reported results accurately reflect real-world deployment conditions. The Inference latency is evaluated as the average time required for processing one facial image, including both image preprocessing, forward propagation to the VGG16 network, and the emotion classification over 10 authentication trials. Both the average inference latency of 24 ms per emotion prediction on the Raspberry Pi 3 B+ satisfy the real-time requirements of interactive authentication and embedded applications.

Table I: The HEBNL Results

Metric / State	Accuracy	TP	Misclassification Rate	FAR	FRR
Happy	99.8 %	99.59 %	0.41 %	0.13 %	0.4 %
Surprise	99.7 %	99.59 %	0.41 %	0.16 %	0.3 %
Normal	98.8 %	98.46 %	1.54 %	0.8 %	1.5 %
Angry	98.9 %	97.77 %	2.23 %	1.5 %	2.2 %

To enable real-time operation on the Raspberry Pi 3 B+, several optimization strategies are adopted on the CRFA module, such as: (i) using the VGG16 backbone in the inference only. (ii) Limiting the emotion recognition to four easily expressible classes led to the reduction of the classification time, and then reduced the computational complexity and latency. (iii) Enhancing the robustness of the system through the HEBNL technique, which aggregates outputs from the best-performing models, avoiding the overhead of parallel inference. As a result, the optimized system achieves an average inference latency of 24 ms per prediction on Raspberry Pi 3 B+, meeting real-time authentication requirements, while its event-driven execution further conserves computational and energy resources.

Another important point is, the proposed system operates in event-driven mode, not continuously, while the authentication is triggered only during the access attempts to the vehicle. This helps to maintain system responsiveness and is well-suited for embedded vehicle security scenarios.

Overall, the system achieves an average accuracy of 98.89%. The system can predict the user's emotions in 24 ms, making it suitable for mobile and IoT devices. HEBNL is evaluated on the KDEF dataset with 10-fold cross-validation. The computed FAR and FRR demonstrate that the system performs exceptionally well across all emotion categories. These results also highlight the model's high precision and recall for these emotional states, suggesting its effectiveness in handling expressive emotions. The CRFA module's FAR and FRR metrics are competitive with other methods, and its integration of liveness detection via emotion challenges provides an additional layer of security. The computational overhead of the CRFA module (VGG16 model combined with HEBNL technique) processes each emotion prediction in approximately 24 ms on the Raspberry Pi 3 B+ hardware. While this latency is suitable for embedded systems, it underscores the trade-off between accuracy and computational demand. The system's total power consumption peaks at 7.5W during active authentication, with an idle state draw of 2.5W.

Although VGG16 is computationally intensive, the fine-tuning process performed on the higher layers reduces the overhead runtime, leading to efficient inference while still preserving the ability to discriminate between different emotions relevant to emotion recognition. The HEBNL technique improves the system robustness by fusing outputs from optimized models without incurring additional inference-time complexity. Furthermore, the emotion classification task was intentionally restricted to four easily expressible emotions, which lowers the classification complexity and inference time compared to full emotion taxonomies. The obtained results show that the CRFA module achieves real-time performance with an average inference latency of 24 ms per prediction and acceptable power consumption, peaking at 7.5 W during the authentication process and remaining low in idle mode. These results indicate that, although VGG16 produces non-negligible computational load, it was still feasible for the deployment for event-driven vehicle access control on the Raspberry Pi 3 B+ hardware, while also highlighting a trade-off between accuracy and efficiency, suggesting that future work may benefit from adopting lightweight CNN architectures to further improve scalability and energy efficiency.

Table 2 shows the comparison and highlights the strengths and weaknesses related to user verification, vehicle tracking, remote control, surveillance, and the proactivity of the system. While most systems, including SMS-based tracking, have theft detection features, IVATS offers additional security measures. IVATS surpasses other systems by incorporating a challenge-response face recognition feature for enhanced user verification. Additionally, IVATS excels in vehicle tracking capabilities. While SMS-based tracking relies on SMS, and LTE-based systems utilize LTE technology for tracking, Real-time Tracking and IVATS offer real-time tracking for precise location information. Remote control functionalities are limited to SMS commands for SMS-based tracking and LTE-based systems, whereas mobile apps provide more comprehensive remote-control options for Real-time Tracking and IVATS. LTE-based systems and Real-time Tracking offer limited proactive measures, and SMS-based tracking lacks proactive security features. As discussed, IVATS introduces proactive elements like challenge-response facial recognition and real-time monitoring. This comparison highlights IVATS as a robust, proactive, and user-friendly anti-theft solution, addressing evolving vehicle security challenges.

Table II: Comparison of the Proposed IVATS System with Existing Vehicle Anti-Theft Systems

Feature	[58]	[51]	[46]	[53]	[27]	[23]	IVATS (proposed)
Theft Detection	Yes	Limited	Yes	Yes	Yes	No	Yes
User Verification	Fingerprint	No	No	No	Face Recognition	Face Recognition	CRFA
Tracking	No	SMS-based	LTE-based	--	--	--	Realtime
Remote Control	Limited (SMS)	Limited (SMS)	Limited (SMS)	--	--		Mobile app
Surveillance	No	No	Camera	Camera	--	--	Camera
Proactive	No	No	Limited	Limited	No	No	Yes
Accuracy of Face Authentication	---	--	--	--	97.41 %	98.2%	98.89%
Cost	--	--	--	50$	--	--	250$

The system scalability is studied based on the following factors:

- **Hardware scalability**: The IVATS system is hardware scalable. It's a Raspberry Pi 3 B+, and the ATmega32 microcontroller provides modular expansion, and sensors integrate without significant redesign. Standard communication protocols (UART, SPI, I2C) for components like GPS, GSM, and cameras allow for easy upgrades. Scaling to thousands of vehicles will require more powerful edge devices, and the GPS/GSM modules are powered by the vehicle's battery.
- **Software scalability**: The CRFA module achieves 98.89% accuracy and processes requests in 24 ms, making it suitable for real-time use. The model can be deployed on a cloud server for centralized processing, and IVATS' normal mode can be activated for low-resource scenarios. A scalable database can be used for storing and querying facial images for a large user base.

Considering the current prices of the shelf components, the IVATS system's total estimated cost is approximately $300. This is calculated from the hardware and software costs, estimated at nearly 200 USD, plus the deployment cost of approximately 100 USD. The energy analysis of IVATS reveals that the Raspberry Pi is the primary power consumer, resulting in 60 Wh/day in standby mode. The system peaks at 7.5W during theft attempts and idles at 2.5W.

While IVATS offers a practical and efficient approach to modern VATS by balancing robustness with user convenience, it remains vulnerable to several potential failure points that could affect its performance:

1) Denied access for the vehicle owner due to complex lighting variations, occlusions, or expression errors in user emotions.
2) Authentication latency from high computational load
3) and network delays of the Raspberry Pi.
4) Inaccurate tracking and delayed alerts or commands due to GSM signal loss from poor satellite visibility.
5) False alarms or failure to detect break-ins caused by sensor malfunction.
6) Loss of remote control due to app crashes or connectivity issues.

The IVATS computational load is primarily driven by its real-time CRFA tasks, which rely on the fine-tuned VGG16 model running on a Raspberry Pi 3B+. It increases processing demands, requiring 24 ms per emotion prediction, which is a feasible but non-negligible latency for embedded hardware. The continuous camera feed processing and cellular data transmission fatigue the Raspberry Pi's limited CPU, risking delays under high concurrency. To mitigate this, future iterations could adopt lightweight models (MobileNetV3, EfficientNet-Lite) or hardware accelerators (Google Coral TPU) to balance speed and accuracy without compromising energy efficiency. To reduce this, future improvements should focus on integrating lightweight models or incorporating hardware accelerators to achieve a balance between speed and accuracy while maintaining energy efficiency.

Because IVATS is a user-dependent behaviour and event-driven system, it is exposed to failure in different scenarios. These scenarios result from realistic vehicle operation conditions and common sources of authentication failure. Specifically, the mentioned evaluations are performed under normal operating conditions to establish a baseline, as well as other reverse conditions that may subject the system to failure, such as (i) low illumination, (ii) partial facial occlusion due to pose or motion variability, and (iii) non-compliant emotional responses. Furthermore, (iv) other failure events may result from authentication retry exhaustion. In addition to the strange use of emotions in authentication, even though the used emotions are simple, the users may find it difficult to cope with the system. The quantitative failure rates of the IVATS system are presented in Table III.

Table III: Qualitative Failure Scenarios of IVATS

Scenario	Failure Rate (%)
Normal conditions	Low
Low illumination	Moderate
Partial occlusion	Higher
Incorrect Emotions	Lower

VII. Conclusion and Future Work

In this paper, an IVATS is proposed as a significant advancement in vehicle security by integrating CRFA, real-time tracking, and proactive theft prevention measures. IVATS leverages a fine-tuned VGG16 model combined with the HEBNL technique to achieve an impressive average accuracy of 98.89% for emotion recognition, ensuring robust and dynamic user verification. Additionally, IVATS incorporates GSM and GPS technologies for seamless communication and precise vehicle localization, while its mobile app provides a user-friendly interface for remote control and monitoring. These contributions address critical gaps in existing VATS, such as reactive responses, unreliable authentication, and limited scalability, positioning IVATS as a comprehensive and innovative solution. Despite its advancements, the IVATS encounters some limitations due to environmental factors, such as poor lighting conditions, which can degrade the performance of the face authentication module, and the computational overhead of the VGG16 model, with a latency of 24 ms per emotion prediction, may strain the Raspberry Pi 3 B+ hardware in high-concurrency scenarios. Furthermore, the system's reliance on GSM networks introduces potential vulnerabilities, including signal loss and delayed alerts.

Future enhancements of the IVATS system will focus on improving computational efficiency by integrating lightweight AI architectures, strengthening facial recognition

robustness under challenging operating conditions. Moreover, large-scale real-world evaluations will be conducted to further validate system performance. Since providing a single deterministic failure rate of the system is a challenge, developing more comprehensive and standardized evaluation methodologies is a motivation.

Acknowledgments

This research paper is not supported by any company or organization; it relies solely on the efforts of the authors.

Competing interests

The authors declare that they have no conflict of interest.

Funding

Not applicable.

Data Availability

The datasets generated and/or analysed during the current study are available from the corresponding author on reasonable request.

Clinical Trial Number

Not applicable.

Consent to Publish

Not applicable.

Ethics and Consent to Participate

Not applicable.

Author Contributions

Ayman Elshenawy: Conceptualization, Methodology, Supervision, and research administration.
Khalil M. Abdelnaby: Software development (Face Recognition algorithms), Data curation, Hardware-software integration, and Literature review.
Mohamed A. Rohaim: Embedded system design (Raspberry Pi configuration), Validation, and Hardware prototyping.
Ayman Mohamed: GPS/GSM module integration (Live Location Tracking), Testing, and Visualization.
Ahmad Shalaldeh: Formal analysis, and Writing – original draft preparation.
Malik AL-Essa: Writing – review & editing, and Final validation.

References

[1] M. Sathiyanarayanan, S. Mahendra, and R. B. Vasu, Smart security system for vehicles using internet of things (IoT), Second International Conference on Green Computing and Internet of Things (ICGCIoT), pp. 41–47, 2018

[2] Z. Liu, A. Zhang, and S. Li, Vehicle anti-theft tracking system based on Internet of things, in Proceedings of 2013 IEEE International Conference on Vehicular Electronics and Safety, 2013, pp. 48–52.

[3] A. Alsaaidah, O. Almomani, A. A. Abu-Shareha, M. M. Abualhaj, and A. Achuthan, ARP Spoofing Attack Detection Model in IoT Networks Using Machine Learning: Complexity vs. Accuracy, Journal of Applied Data Sciences, vol. 5, no. 4, pp. 1850 – 1860, 2024, https://doi.org/10.47738/jads.v5i4.374.

[4] A. Akhunzada, A. S. Al-Shamayleh, S. Zeadally, A. Almogren, and A. A. Abu-Shareha, Design and performance of an AI-enabled threat intelligence framework for IoT-enabled autonomous vehicles, Computers and Electrical Engineering, vol. 119, 2024, https://doi.org/10.1016/j.compeleceng.2024.109609.

[5] N. Moawad, T. Heggi, S. F. Ellakwa, M. M. H. Gad El-Moula, and A. Mohamed, "An Intelligent System for Optimizing Irrigation Water Usage for Cucumber Crop in Egypt General Terms," 2024.

[6] T. J. Claude, I. Viviane, I. J. Paul, and M. Didacienne, "Development of Security Starting System for Vehicles Based on IoT," in 2021 International Conference on Information Technology (ICIT), 2021, pp. 505–510.

[7] Tejashwini and S. K. Panda, "Design and Development of Vehicle Theft Detection, Tracking and Accident Identifier System using IoT," Journal of University of Shanghai for Science and Technology, vol. 23, no. 7, 2021.

[8] S. T. Ali et al., "Design and Implementation of an Integrated Vehicle Security System (IVSS)," International Journal of Industry and Sustainable Development (IJISD), vol. 3, no. 1, 2022, http://ijisd.journals.ekb.eg

[9] Raihan Ahmed Joy, Md. Amanullah Sarker, and Md. Nazmul Hasan Sarker, "Design and implementation of vehicle location tracking system for University Bus Developing Android Application," World Journal of Advanced Research and Reviews, vol. 20, no. 2, pp. 441–453, Nov. 2023, https://doi.org/10.30574/wjarr.2023.20.2.2197.

[10] S. Paing, M. Oo, M. Othman, and N. Funabiki, "A Personal Use Vehicle Anti-Theft Tracking System Using IoT Platform," International Journal of Computer & Software Engineering, vol. 4, no. 1, Jan. 2019. https://doi.org/10.15344/2456-4451/2019/141

[11] A. M. Marathe, M. S. Samak, and M. S. Kulkarni, "Third Party AntiTheft Automobile Security System," International Journal on Recent and Innovation Trends in Computing and Communication, vol. 2, no. 3, Mar. 2014, http://www.ijritcc.org

[12] J. Arellano-Zubiate, J. Izquierdo-Calongos, A. Delgado, and E. L. Huamaní, "Vehicle Anti-Theft Back-Up System using RFID Implant Technology," International

Journal on Recent and Innovation Trends in Computing and Communication, vol. 10, no. 5, pp. 36–40, May 2022, https://doi.org/10.17762/ijritcc.v10i5.5551

[13] V. Srinivasarao, D. Mahendra, K. L. Chaitanya, B. H. Sai, and D. R. Rohan, "A NOVEL VEHICLE SECURITY SYSTEM USING DRIVER'S LICENSE AND FINGERPRINT AUTOMATION," Journal of Nonlinear Analysis and Optimization, vol. 15, no. 1, pp. 300–311, 2024.

[14] A. T. Noman, S. Hossain, S. Islam, M. E. Islam, N. Ahmed, and M. A. M. Chowdhury, "Design and implementation of microcontroller based antitheft vehicle security system using GPS, GSM and RFID," in 2018 4th International Conference on Electrical Engineering and Information & Communication Technology (iCEEiCT), 2018, pp. 97–101.

[15] B. Sombo, S. Tooswem, E. Olaye, J. Falilat, and L. Adewale, "Development of a secured ignition and notification for an anti-theft vehicle detection system using on-time password," 2024.

[16] M. Chaabane, H. Chaibi, A. Elrharras, R. Saadane, A. Chehri, and A. Jakimi, "Vehicle Anti-Theft Systems Using Vision Transformer and Iris Identification," in Lecture Notes in Networks and Systems, Springer Science and Business Media Deutschland GmbH, 2024, pp. 222–234. https://doi.org/10.1007/978-3-031-74491-4_18.

[17] A. A. Elkhail, R. U. D. Refat, R. Habre, A. Hafeez, A. Bacha, and H. Malik, "Vehicle Security: A Survey of Security Issues and Vulnerabilities, Malware Attacks and Defenses," IEEE Access, vol. 9, pp. 162401–162437, 2021, https://doi.org/10.1109/ACCESS.2021.3130495.

[18] X. Zhou and T. C. Zhu, "Survey of Research on Face Recognition Methods Based on Depth Learning," in Journal of Physics: Conference Series, Institute of Physics, 2024. https://doi.org/10.1088/1742-6596/2717/1/012027.

[19] Y. Kortli, M. Jridi, A. Al Falou, and M. Atri, "Face recognition systems: A survey," Jan. 02, 2020, MDPI AG. https://doi.org/10.3390/s20020342.

[20] S. Balasubramanian, A. Ingle, N. Joshi, S. Kushwaha, and M. R. Naik, "A review study on Vehicle Anti-Theft Immobilization System using Face Recognition," International Research Journal of Engineering and Technology, vol. 09, no. 10, pp. 1082–1087, Oct. 2022, www.irjet.net

[21] V. Parmar, R. Shinde, S. Agrawal, and N. Meshram, "Vehicle Anti-Theft Face Recognition System Using Raspberry Pi," International Journal of Science, Engineering and Technology, pp. 2–4, 2021.

[22] V. S. Katti, D. Sweshitha, S. K. Mahendra, and S. M. Akash, "Anti-Theft Face Recognition and Alcohol Detection Car Ignition System," in 2023 IEEE Women in Technology Conference (WINTECHCON), 2023, pp. 1–6.

[23] A. A. Elngar and M. Kayed, "Vehicle Security Systems using Face Recognition based on Internet of Things," Open Computer Science, vol. 10, no. 1, pp. 17–29, Jan. 2020, https://doi.org/10.1515/comp-2020-0003.

[24] B. Balakrishnan, P. Suryarao, R. Singh, S. Shetty, and S. Upadhyay, "Vehicle anti-theft face recognition system, speed control and obstacle detection using raspberry pi," in 2022 IEEE 5th International Symposium in Robotics and Manufacturing Automation (ROMA), 2022, pp. 1–5.

[25] S. Omer, K. Sohelrana, A. Tamkeen, M. A. Rasheed, and others, "Real time application of vehicle anti theft detection and protection with shock using facial recognition and iot notification," in 2020 Fourth International Conference on Computing Methodologies and Communication (ICCMC), 2020, pp. 1039–1044.

[26] S. Fasiuddin, S. Omer, K. Sohelrana, A. Tamkeen, and M. A. Rasheed, "Real Time Application of Vehicle Anti Theft Detection and Protection with Shock Using Facial Recognition and IoT Notification," in Proceedings of the 4th International Conference on Computing Methodologies and Communication, ICCMC 2020, Institute of Electrical and Electronics Engineers Inc., Mar. 2020, pp. 1039–1044. https://doi.org/10.1109/ICCMC48092.2020.ICCMC-000194.

[27] V. Viswanatha, A. Hebbar, N. Anand, and A. Kumar, "AI-Enabled Smart Vehicle with CNN and Deep Face for Anti-Theft Detection System," in 2024 1st International Conference on Software, Systems and Information Technology, SSITCON 2024, Institute of Electrical and Electronics Engineers Inc., 2024. https://doi.org/10.1109/SSITCON62437.2024.10796070.

[28] P. Langde, S. Bhowate, N. Dharpure, P. Gajbhiye, K. B. Student, and S. P. Student, "ANTI-THEFT VEHICLE SECURITY SYSTEM USING FACE RECOGNITION," Journal of Emerging Technologies and Innovative Research (JETIR), vol. 8, no. 5, pp. 108–111, 2021, www.jetir.orgd108.

[29] D. Pandrangi, S. Vinod, S. Nagaraju, and L. Surendra, "VEHICLE ANTI THEFT DETECTION AND PROTECTION WITH SHOCK USING FACIAL RECOGNITION," Journal of Nonlinear Analysis and Optimization, vol. 15, no. 1, 2024.

[30] A. Idris, M. N. Iman, S. M. Sulong, W. N. W. Muhamad, and A. A. Bakar, "Vehicle Tracking System Based on Internet of Things Utilizing TTGO T-CALL ESP32 SIM800l," Journal of Advanced Research in Applied Sciences and Engineering Technology, vol. 45, no. 2, pp. 118–127, Mar. 2025, https://doi.org/10.37934/araset.45.2.118127.

[31] Dhanya NM, "Anti-Theft Vehicle Tracking System Using GPS and Location Prediction," International Journal on Advanced Science, Engineering and Information Technology (IJASEIT), vol. 8, no. 6, 2018, https://docs.google.com/spreadsheets/d/1cwXq

[32] S. Nairouz, R. Dashti, Z. B. Abbas, A. Alajmi, H. Almutairi, and M.Rashdan, "Vehicle Anti-Theft Security System with GPS Tracking and Remote Engine Locking," in 2023 5th International Conference on Bioengineering for Smart Technologies (BioSMART), 2023, pp. 1–5.

[33] A. A. Abdirahman, A. O. Hashi, U. M. Dahir, M. A. Elmi, and S. Z. M. Hashim, "Enhanced Vehicle Tracking: A GPS-GSM-IoT Approach," International Journal of Computing and Digital Systems, vol. 17, no. 1, pp. 1–11, Jun. 2025, https://doi.org/10.12785/ijcds/1571012134.

[34] N. A. Zulkifli and S. Mohd Shah, "Three-Level Car Security System with GPS Tracker Using IoT," Journal of Electronic Voltage and Application, vol. 4, no. 1, Oct. 2023, https://doi.org/10.30880/jeva.2023.04.01.004.

[35] H. M. Marhoon, A. I. Alanssari, and N. Basil, "Design and Implementation of an Intelligent Safety and Security System for Vehicles Based on GSM Communication and IoT Network for Real-Time Tracking," Journal of Robotics and Control (JRC), vol. 4, no. 5, pp. 708–718, 2023, https://doi.org/10.18196/jrc.v4i5.19652.

[36] M. Aiman, M. Sharif, N. M. Suhaimi, and M. A. Zakaria, "Analysis of GPS and GSM with GPRS-Based Vehicle Tracking and Monitoring System," JOURNAL OF MECHATRONICS AND INTELLIGENT MANUFACTURING, vol. 6, no. 1, pp. 38–43, May 2024, https://doi.org/10.15282/mekatronikajintellmanufmechatron.v6i1.10744.

[37] Z. Y. Huang et al., "A study on computer vision for facial emotion recognition," Sci Rep, vol. 13, no. 1, Dec. 2023. https://doi.org/10.1038/s41598-023-35446-4.

[38] O. Kalyta, O. Barmak, P. Radiuk, and I. Krak, "Facial Emotion Recognition for Photo and Video Surveillance Based on Machine Learning and Visual Analytics," Applied Sciences (Switzerland), vol. 13, no. 17, Sep. 2023, https://doi.org/10.3390/app13179890.

[39] S. Shamili Shanmugapriya, S. V Anila, D. Hemalatha, K. Karthika, V. Sankaradass, and S. Singh, "Optimizing Security Posture via Synergized Fingerprint and Facial Recognition in Integrated Authentication Framework," in 2024 International Conference on Advances in Data Engineering and Intelligent Computing Systems (ADICS), 2024, pp. 1–5. https://doi.org/10.1109/ADICS58448.2024.10533559.

[40] Y. An, J. Lee, E. S. Bak, and S. Pan, "Deep Facial Emotion Recognition Using Local Features Based on Facial Landmarks for Security System," Computers, Materials and Continua, vol. 76, no. 2, pp. 1817–1832, Aug. 2023, https://doi.org/10.32604/cmc.2023.039460.

[41] M. Ezz, A. M. Mostafa, and A. Elshenawy, "Challenge-Response Emotion Authentication Algorithm Using Modified Horizontal Deep Learning," Intelligent Automation and Soft Computing, vol. 35, no. 3, pp. 3659–3675, 2023, https://doi.org/10.32604/iasc.2023.031561.

[42] P. Ghadekar, M. Ranjan Pradhan, D. Swain, and B. Acharya, "EmoSecure: Enhancing Smart Home Security with FisherFace Emotion Recognition and Biometric Access Control," IEEE Access, vol. 12, pp. 93133–93144, 2024, https://doi.org/10.1109/ACCESS.2024.3423783.

[43] C. S. Pillai, R. Pedram, N. Salumuri, D. Nath, and K. Pakhrani, "ParkShield: Two-Wheeler Anti-Theft System," in 2022 6th International Conference On Computing, Communication, Control And Automation (ICCUBEA, 2022, pp. 1–5.

[44] S. S. Chakole and N. A. Ukani, "Low power smart vehicle tracking, monitoring, collision avoidance and antitheft system," in 2020 Second International Conference on Inventive Research in Computing Applications (ICIRCA), 2020, pp. 1096–1101.

[45] K. Shruthi, P. Ramaprasad, R. Ray, M. A. Naik, and S. Pansari, "Design of an anti-theft vehicle tracking system with a smartphone application," in 2015 International Conference on Information Processing (ICIP), 2015, pp. 755–760.

[46] M. S. Taha, A. A.-A. Haddad, N. A. Y. Alrashdi, M. H. Mahdi, H. N. Khalid, and Q. J. Yousif, "An advance vehicle tracking system based on Arduino electronic shields and web maps browser," in 2021 International Conference on Advanced Computer Applications (ACA), 2021, pp. 238–243.

[47] Z. Wang, J. Mo, C. Zhao, Q. Wang, and K. Wang, "Dynamic modeling and brake stick-slip vibration analysis of a vehicle-track system with disc-pad nonlinear frictions," Tribol Int, vol. 202, p. 110317, 2025.

[48] G. Yang, Z. Chen, Z. Chen, J. Yang, and W. Zhai, "Dynamic investigation of a rack vehicle–track coupled system considering effect of multi-stage gear transmissions," Nonlinear Dyn, vol. 113, no. 9, pp. 9509–9528, 2025.

[49] G. Li, X. Wang, S. Wu, L. Ma, W. Ding, and others, "Dynamic response analysis of vehicle-track coupled system at subgrade-bridge transition zone in seasonal frozen region under multi-source excitation," Soil Dynamics and Earthquake Engineering, vol. 190, p. 109216, 2025.

[50] R. Jain, P. Raizada, A. K. Kushwaha, R. Bhatnagar, and S. Saboo, "Blind Vision and Theft Protection Device in Vehicles using Embedded Systems," in 2021 International Conference on Smart Generation Computing, Communication and Networking (SMART GENCON), 2021, pp. 1–6.

[51] K. J. Prakash, K. P. K. Reddy, K. S. K. Goud, and S. T. Reddy, "Vehicle theft intimation over sms and remote control of its engine," in 2021 6th International Conference on Communication and Electronics Systems (ICCES), 2021, pp. 1496–1501.

[52] R. Roupesh, M. Swatha, M. Jagadeeswari, S. Padmapriya, and others, “Anti-Theft Alarm System and Tracking in Coal Mines,” in 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), 2023, pp. 653–657.
[53] T. Islam, M. J. U. Qureshi, H. Palit, and M. A. Sayeed, “Design and Implementation of a Two-Step Security System for Cargo Vehicles Theft Prevention and Real-time Monitoring through IoT,” in 2023 14th International Conference on Computing Communication and Networking Technologies (ICCCNT), 2023, pp. 1–6.
[54] P. N. Renjith, S. Balasubramani, K. Ramesh, and E. Patnala, “An Initial Risk Assessment for Multimodal with LSTM-Based Trust Evaluation Framework for Autonomous Vehicle Security,” SN Comput Sci, vol. 6, no. 2, pp. 1–15, 2025.
[55] I. A. Khan et al., “A context-aware zero trust-based hybrid approach to IoT-based self-driving vehicles security,” Ad Hoc Networks, vol. 167, p. 103694, 2025.
[56] R. Brooks, I. Aideyan, and M. Pese, “Security and data privacy of modern automobiles,” in Data Analytics for Intelligent Transportation Systems, Elsevier, 2025, pp. 141–184.
[57] R. P. Mahesh and R. Imdad, “IoT-Based Embedded System for Vehicle Security And Driver Surveillance,” in Proceedings of the 2nd International Conference on Inventive Communication and Computational Technologies (ICICCT 2018), IEEE Explore Compliant-Part Number: CFP18BAC-ART, 2018.
[58] M. J. Raj, S. Gadde, and R. Jayaraman, “Implementation of biometric access control using fingerprint for safety and security system of electric vehicle,” in 2021 2nd International Conference on Smart Electronics and Communication (ICOSEC), 2021, pp. 1684–1689.
[59] V. Srinivasarao, D. Mahendra, K. L. Chaitanya, B. H. Sai, and D. R. Rohan, “A NOVEL VEHICLE SECURITY SYSTEM USING DRIVER’S LICENSE AND FINGERPRINT AUTOMATION,” Journal of Nonlinear Analysis and Optimization, vol. 15, no. 1, 2024.
[60] A. K. Singh, M. Dhawan, E. D. Sharma, and S. Kumar, “Advance AntiTheft Flooring Security System using Raspberry PI,” in 2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET), 2023, pp. 1–5.
[61] Y. Srinivas, K. Vinay, M. Arjun, M. Rohith, N. Harikrishna, and others, “Fingerprint Based Vehicle Anti-Theft Detection and Alerting System,” in 2023 7th International Conference on Electronics, Communication and Aerospace Technology (ICECA), 2023, pp. 929–934.
[62] K. Jeevitha, J. Venkatesh, V. Indhumathi, K. K. Veni, R. P. Kumar, and others, “A Biometric Vehicle Theft Identification and Prevention Scheme using GPS Location Tracking,” in 2023 International Conference on Advances in Computing, Communication and Applied Informatics (ACCAI), 2023, pp. 1–8.
[63] R. J. Teradal, S. J. Chougule, S. N. Chopade, A. B. Chougule, V. Dalal, and S. S. Atiwadkar, “Comprehensive IoT-Based Vehicle Security: License Verification and Biometric Authentication,” in 2025 6th International Conference on Mobile Computing and Sustainable Informatics (ICMCSI), 2025, pp. 226–233.
[64] H. Shin, W. Park, S. Kim, J. Kweon, and C. Moon, “Driver Identification System Based on a Machine Learning Operations Platform Using Controller Area Network Data,” Electronics (Basel), vol. 14, no. 6, p. 1138, 2025.
[65] W. Wang, S. Zhang, G. Liu, and Y. Zhao, “A Blockchain-Based CrossDomain Authentication Scheme for Unmanned Aerial Vehicle-Assisted Vehicular Networks,” World Electric Vehicle Journal, vol. 16, no. 4, p. 199, 2025.
[66] M. Dey, M. A. Arif, and M. A. Mahmud, “Anti-theft protection of vehicle by GSM & GPS with fingerprint verification,” in 2017 International Conference on Electrical, Computer and Communication Engineering (ECCE), 2017, pp. 916–920.
[67] J. Singh, D. Virk, and others, “Bluetooth Enabled Anti-Theft System Using Android Based Handheld Device,” in 2018 6th Edition of International Conference on Wireless Networks & Embedded Systems (WECON), 2018, pp. 122–125.
[68] M. Qian, H. Gao, and W. Liu, “Android based vehicle anti-theft alarm and tracking system in hand-held communication terminal,” in 2018 IEEE International Conference on Consumer Electronics-Taiwan (ICCE-TW), 2018, pp. 1–2.
[69] K. Lappanitchayakul, “Anti-theft device for car: Alert system using radio wave,” in 2019 International Conference on Intelligent Informatics and Biomedical Sciences (ICIIBMS), 2019, pp. 351–355.
[70] A.-V. Palacean, D.-C. Trancă, C. Contaşel, R. Tătăroiu, and C. Dutescu, “IoT Enabled Optimized Architectures for GPS Anti-Theft Tracking Devices,” in 2021 20th RoEduNet Conference: Networking in Education and Research (RoEduNet), 2021, pp. 1–6.
[71] R. Vinaykumar, K. Bajid, D. S. Hemalatha, S. M. Patil, and V. Raman, “Advanced Features for Electric Vehicle: The Future Smart Transportation,” in 2023 International Conference on Recent Advances in Science and Engineering Technology (ICRASET), 2023, pp. 1–4.
[72] K. Thamoethata, B. Isong, N. Dladlu, and A. M. Abu-Mahfouz, “Analysis of IoT-based vehicle anti-theft security,” in 2021 3rd International Multidisciplinary Information Technology and Engineering Conference (IMITEC), 2021, pp. 1–6.
[73] S. Zhang, “Design of intelligent anti electricity theft monitoring device based on ARM computing modeling,” International Journal of Emerging Electric Power Systems, 2025.

[74] Y. Hu, R. Wu, G. Li, Z. Shen, and J. Xie, "Facial Features Controlled Smart Vehicle for Disabled/Elderly People," Electronics (Basel), vol. 14, no. 6, p. 1088, 2025.
[75] M. Vandabona, V. Gnanaraj, M. Attygala, D. Kumar, and A. Jolfaei, "Sensors and security considerations for emergency vehicles," in Sensor Networks for Smart Hospitals, Elsevier, 2025, pp. 435–452.
[76] D. Lundqvist, A. Flykt, and A. Öhman, "Karolinska directed emotional faces," Cogn Emot, 1998.



Ayman Elshenawy earned his Ph.D. in Systems and Computer Engineering from Al-Azhar University in Egypt in 2013. He is currently a professor in the Networks and Cybersecurity Department at the Faculty of Information Technology, Al-Ahliyya Amman University, Amman, Jordan. In parallel, he serves as a full professor in the Systems and Computer Engineering Department, Faculty of Engineering, Al-Azhar University, Egypt, and as an Associate Professor at both the Egyptian Chinese University (ECU) and the Innovation University (IU), Egypt. His research interests span a wide range of areas, including cloud robotics, educational machine learning, deep learning applications in security, software engineering, hardware Trojan detection, and natural language processing. He has made notable contributions to these fields, with publications in high-quality journals and conferences such as The Computer Journal, International Journal of Imaging and Robotics, Wireless Personal Communications, Education and Information Technologies, International Journal of Advanced Computer Science and Applications, Journal of Information Technology Management, Intelligent Automation and Soft Computing, International Journal of Information Technology (Singapore), International Review of Automatic Control (IREACO), Scientific Reports, and IEEE Access. He is also an active participant in several IEEE conferences. E-mail: a.elshenawy@ammanu.edu.jo
ORCID: https://orcid.org/0000-0002-1309-6449



Khalil M. Abdelnaby is an associate professor of Data Science, Artificial Intelligence Department, Faculty of Information Technology, Al-Ahliyya Amman University at Amman, Jordan. He received his M.Sc. and Ph.D. degrees in systems and computers engineering Dept. from Al-Azhar University in 2015 and 2019, respectively.
His fields of interest include Artificial Intelligence, Smart Systems, Deep Learning, Data Mining, Mathematics, Robotics, Automotive Control Systems, Motion and Navigation Control, LLM Acceleration with FPGA, and Embedded systems for IoT signal processing.
Email: k.abdelnaby@ammanu.edu.jo
ORCID: http://orcid.org/0000-0002-7482-1392



Mohamed A. Rohaim is an Assistance Professor of Data Science, Artificial Intelligence Department, Faculty of Information Technology, Al-Ahliyya Amman University at Amman, Jordan. He received his M.Sc. and Ph.D. degrees in systems and computers engineering Dept. from Al-Azhar University in 2010 and 2015, respectively. His fields of interest include Artificial Intelligence, Deep Learning, Data Mining and Arabic natural language processing.
Email: m.rohaim@ammanu.edu.jo
ORCID: https://orcid.org/0009-0002-0949-8928



Ayman Mohamed received a Bachelor of Science (Scientific Computing) from Zagazig University, Egypt, a Master of Information Systems, Institute of Computer Science and Artificial Intelligence from Helwan University, Egypt, and a Ph.D. in the Information System Department with the Title "Intelligent Decision Support System Approach to Mitigate Climate Change Effects", Helwan University, Egypt. He was the Vice Dean for Student Affairs at Badya University. Currently, he is an Assistant Professor in the Faculty of Information Technology, Data Science and Artificial Intelligence Department, Al-Ahliyya Amman University, Amman, Jordan. His research interests are Decision Support Systems, Expert Systems, and Artificial Intelligence. In addition, he has actively participated in IEEE conferences on International Information Technology and Artificial Intelligence. He can be contacted at email: a.mohamed@ammanu.edu.jo. He works as a Researcher at the Agricultural Research Center (ARC), email: a.mohamed@arc.sci.eg
ORCID: https://orcid.org/0000-0001-6900-4892



Ahmad Shalaldeh is with the Department of Data Science and Artificial Intelligence, Faculty of Information Technology, Al-Ahliyya Amman University, Amman 19111, Jordan. His research interests include image processing, machine learning, deep learning, and neural networks. He has published several papers applying artificial intelligence techniques in agriculture and animal science.
Email: a.shalaldeh@ammanu.edu.jo
ORCID: https://orcid.org/0000-0001-6171-7150)



Malik AL-Essa has a Ph.D. in Computer Science. Currently works as a lecturer in the Computer Science Department at King Abdull II School for Information Technology, University of Jordan, Jordan. His research interests include Cybersecurity, IDS, and XAI. He can be contacted at this email: m.alessa@ju.edu.jo.