Karafan
Quarterly Scientific Journal of National University of Skill
Spring 2026, Vol. 23, No. 1, p. 13-30
Journal Homepage: https://karafan.tvu.ac.ir/?lang=en
doi: 10.48301/kssa.2025.500797.3124

Design and Construction of a Multi-Layer Anti-Theft Security System for Vehicles

Bahman Rahmatinejad[1*], Hossein Rahimi Asiabaraki[2*], Farzin Azimpour Shishevan[3], Hadi Ghasemi Zavaregh [4],

[1,2,3,4] Department of Mechanical Engineering, Technical and Vocational University (TVU), Tehran, Iran.

ARTICLE INFO

Article Type:
Original Research

Received: 24.01.2025
Revised: 02.04.2025
Accepted: 14.12.2025

Keyword:
Anti-Theft System
Fingerprint
Coded Start
Arduino
RFID

[*]Corresponding Author:
Bahman Rahmatinejad &
Hossein Rahimi Asiabaraki
Email:
brahmati@tvu.ac.ir
h.rahimi@tvu.ac.ir

ABSTRACT

The pressure from automobile insurance companies, along with the concerns of vehicle owners and the increasing rate of theft and the sophistication of car thieves, has prompted designers and manufacturers to come up with new designs and ideas for anti-theft systems every day. In this research, a three-layer security system was designed and a prototype was built. The Arduino microcontroller was used for programming. Additionally, biometric fingerprint recognition, RFID technology, and a keypad for code entry were employed to activate the system. The results showed that the RFID system, with an average of 2.4 seconds, was the fastest method, while fingerprint scanning took 3.7 seconds, making it the slowest method for information retrieval by the Arduino board. Overall, the designed three-layer system requires 9.76 seconds to activate. In this electronic circuit, the activation of the switch, waking up the ECU, operating the fuel pump, and starting the ignition can be contingent upon receiving this information. The system will remain inactive until the correct information from the three security layers is entered. After design, this system was installed on an inline four-cylinder engine and numerous field tests were conducted under real conditions to evaluate its performance.

©2024 the authors. Published by National University of Skills, Tehran, Iran. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution-Noncommercial 4.0 International (CC BY-NC License) (https://creativecommons.org/licenses/by-nc/4.0/)

E-ISSN: 2538-4430
ISSN: 2382-9796

EXTENDED ABSTRACT

Introduction

Vehicle theft remains a critical concern for owners and insurance companies. In Iran alone, tens of thousands of vehicles are stolen annually, with an average theft time of less than 2.5 minutes. Approximately 40% of all recorded thefts involve motor vehicles. This research presents a novel three-layer hybrid security system. The main innovation lies in intelligently combining three independent authentication methods: fingerprint biometric recognition, RFID technology, and keypad-based code entry. The system is programmed using an Arduino microcontroller. The electronic circuit is architected such that critical vehicle processes (switch activation, ECU wake-up, fuel pump operation, and ignition initiation) are enabled only upon successful verification of all three layers. Following design, the system was installed on a four-cylinder inline engine and subjected to multiple field tests under real-world conditions.

Materials and methods

Initially, a database containing fingerprint data, RFID cards, and keypad codes is created. To start the engine, the user first places their finger on the biometric fingerprint scanner. The Arduino processes the data and verifies it against the database. If correct, the system proceeds to the RFID reader. The RFID module scans the card; if the data matches, the system proceeds to the keypad. The user then enters a predefined numeric passcode. If all three steps are successful, a relay activates and the engine starts (Figure 1).

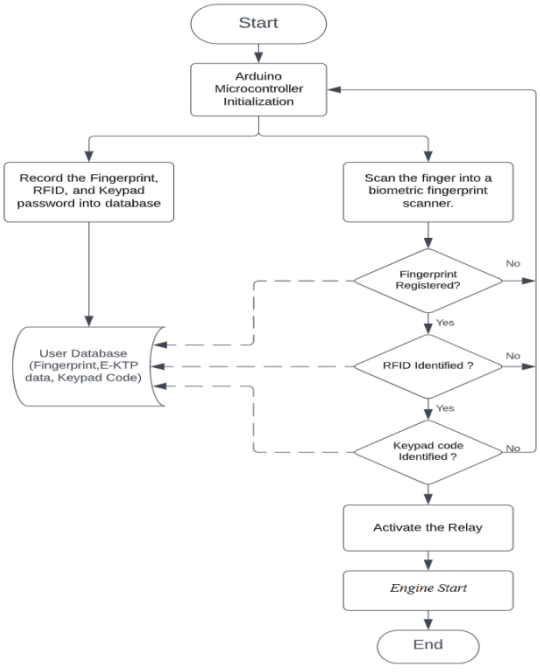


Figure 1. Flowchart of the authentication process for the three-layer anti-theft system

Fingerprint sensor-based authentication mechanism

Biometric identification systems utilize individuals' unique physiological characteristics. Fingerprint recognition was selected due to its high accuracy, pattern uniqueness, cost-effectiveness, and ease of integration. The fingerprint sensor provides initial identification. The Arduino then outputs a voltage indicating whether the fingerprint is accurate. If correct, the process proceeds to the RFID reader.

RFID card-based authentication mechanism

The RC522 RFID Reader module (operating at 13.56 MHz) generates an electromagnetic field. When an RFID tag enters this field, it becomes activated and transmits data via radio pulses. The reader receives and processes this data. Upon successful verification, Arduino pin 7 activates relay pin 85, redirecting current to power the fuel pump, starter, ignition system, and injectors. Once activated, the system allows a 5-minute window for engine start before requiring re-authentication.

Activation code-based authentication mechanism

A numeric keypad is used for entering a predefined activation code. The system compares the entered code with the stored code. After three consecutive incorrect attempts, an alarm buzzer activates for 20 seconds.

The final prototype board uses an electromotor as a performance indicator instead of an actual fuel pump, starter, and injectors. The RFID module and fingerprint sensor operate at 3.3V, while the keypad, LCD (16x2), I2C, buzzer, and relays require 5V. The electromotor (simulating the vehicle system) requires 9V and 12V. This multi-voltage architecture ensures coordinated operation of all components.

Results and discussion

To evaluate system performance, ten repeated measurements were conducted for each authentication layer. Table 1 presents the response times for fingerprint scanning, RFID card reading, and activation code analysis.

Table 1. Time required for each authentication mechanism

Test No.	Fingerprint (s)	RFID (s)	Keypad Code (s)
1	3.6	2.0	3.6
2	3.8	2.2	3.8
3	3.5	2.5	3.5
4	3.7	2.1	3.7
5	3.9	2.2	3.9
6	3.8	2.6	3.5
7	3.7	2.4	3.7
8	3.6	2.9	3.8
9	3.9	2.4	3.5
10	3.5	2.7	3.6
Average	3.7	2.4	3.66

The results show that the RFID layer demonstrated the fastest response time (2.4 seconds), while fingerprint scanning was the slowest (3.7 seconds). The keypad code analysis required 3.66 seconds. The total authentication time for all three layers is 9.76 seconds. System stability was confirmed with timing variations below 0.5 seconds per layer across all tests. As shown in Figure 2, the RFID layer was fastest and fingerprint scanning slowest.

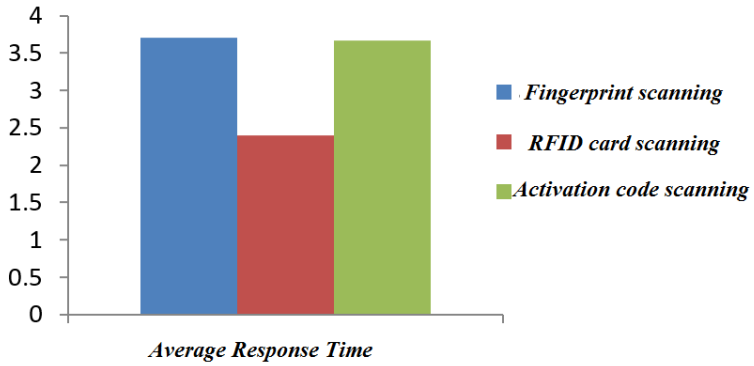


Figure 2. Average response time of each authentication mechanism (fingerprint, RFID, and keypad)

Field tests on a four-cylinder inline engine confirmed that the system effectively prevents unauthorized engine activation when any authentication layer fails (including fingerprint mismatch, unauthorized RFID cards, or incorrect code entry). The system performed without failure across all test scenarios, demonstrating high reliability. Compared to industrial standards, this performance is within acceptable ranges, maintaining high security with practical response speeds.

Conclusion

This research successfully designed and constructed a multi-layer vehicle anti-theft security system combining fingerprint biometrics, RFID technology, and numeric keypad authentication using an Arduino microcontroller. The RFID system was fastest (2.4 s average), while fingerprint scanning was slowest (3.7 s average). The keypad code analysis required 3.66 seconds. Total system activation requires 9.76 seconds. The electronic circuit can condition switch activation, ECU wake-up, fuel pump operation, and ignition initiation upon successful verification of all three layers. The system prevents activation until correct information is received from all layers. Field tests on a four-cylinder inline engine confirmed effective prevention of unauthorized access. This novel solution offers a multi-layer security approach with appropriate response times, representing an effective step toward enhancing vehicle security with high potential for automotive industry applications.

کارافن
فصلنامه علمی دانشگاه ملی مهارت
بهار ۱۴۰۵، دوره ۲۳، شماره ۱، ۳۰-۱۳
آدرس نشریه: https://karafan.tvu.ac.ir
doi :10.48301/kssa.2025.500797.3124

طراحی و ساخت سیستم چندلایه امنیتی ضدسرقت خودرو

بهمن رحمتی‌نژاد[1*]، حسین رحیمی آسیابرکی[2*]، فرزین عظیم‌پور شیشوان[3]، هادی قاسمی زوارق[4]

۱و۲و۳و۴- گروه مهندسی مکانیک، دانشگاه ملی مهارت، تهران، ایران.

اطلاعات مقاله

نوع مقاله: مقاله پژوهشی

دریافت مقاله: ۱۴۰۳/۱۱/۰۵
بازنگری مقاله: ۱۴۰۴/۰۱/۱۳
پذیرش مقاله: ۱۴۰۴/۰۹/۲۳

کلید واژگان:
سیستم ضد سرقت
اثرانگشت
استارت کددار
آردوینو
RFID

***نویسنده مسئول:**
بهمن رحمتی‌نژاد و حسین رحیمی آسیابرکی
پست الکترونیکی:
brahmati@tvu.ac.ir
h.rahimi@tvu.ac.ir

چکیده

فشار کمپانی‌های بیمه‌کننده خودرو و همچنین نگرانی صاحبان وسایل نقلیه خودرویی و همین‌طور افزایش سرقت و مهارت یافتن سارقان خودرو، طراحان و سازندگان را بر آن داشته تا هرروز طرحی نو و ایده‌ای نو در زمینه سیستم‌های ضدسرقت طراحی کنند. در این پژوهش یک سیستم امنیتی سه‌لایه طراحی و نمونه اولیه آن ساخته شد. به‌منظور برنامه‌نویسی از میکروکنترلر آردوینو و برای فعال شدن سیستم از روش شناسایی بیومتریک اثرانگشت، تکنولوژی RFID و صفحه‌کلید جهت واردکردن کد فعال‌سازی استفاده شد. نتایج نشان داد سیستم RFID با میانگین ۲,۴ ثانیه سریع‌ترین روش و اسکن اثرانگشت با ۳,۷ ثانیه کندترین روش در دریافت اطلاعات توسط برد آردوینو است. در مجموع سیستم سه‌لایه طراحی‌شده جهت فعال شدن نیاز به ۹,۷۶ ثانیه زمان دارد. در این مدار الکترونیکی می‌توان فعال شدن سوئیچ، بیدار شدن ECU، کار کردن پمپ‌بنزین و همچنین شروع جرقه‌زنی را منوط به دریافت این اطلاعات نمود و تا زمانی که اطلاعات صحیح از سه‌لایه امنیتی دریافت نشود، از فعال شدن سیستم جلوگیری کرد. این سیستم بعد از طراحی بر روی یک موتور چهار سیلندر خطی نصب و آزمایش‌های میدانی متعددی در شرایط واقعی به‌منظور ارزیابی عملکرد آن انجام شد.

شاپای الکترونیکی: ۲۵۳۸-۴۴۳۰
شاپای چاپی: ۲۳۸۲-۹۷۹۶

©2024 the authors. Published by National University of Skills, Tehran, Iran. This article is an open-access article distributed under the terms and conditions of the Creative Commons Attribution-Noncommercial 4.0 International (CC BY-NC License) (https://creativecommons.org/licenses/by-nc/4.0/)

مقدمه

استفاده از وسایل نقلیه برای حمل بار، جابجایی مسافر و سایر امور مرتبط، ضرورتی اجتناب‌ناپذیر در زندگی مدرن به شمار می‌رود. این امر به نوبه خود موجب بروز جرائم مرتبط با وسایل نقلیه، به‌ویژه سرقت، شده است. در میان انواع جرائم، سرقت وسایل نقلیه به‌عنوان یک عمل عمدی و سازمان‌یافته، علاوه بر اهداف مالی، اغلب برای استفاده از خودروهای سرقتی در ارتکاب جرائم دیگر مانند اعمال خرابکارانه، جرائم امنیتی، قتل، سرقت‌های مسلحانه و غیره صورت می‌پذیرد [۱]. سرقت خودرو ازجمله جرائمی است که در مقایسه با سایر جرائم، با فراوانی بیشتری اتفاق می‌افتد. پیامدهای ناگوار این جرم نه‌تنها موجب ایجاد احساس ناامنی در جامعه می‌شود، بلکه مشکلات متعددی را برای مالباختگان به وجود می‌آورد. از سوی دیگر، تنوع مدل‌های خودروهای داخلی و خارجی، استفاده گسترده از آن‌ها توسط مردم و سطح ایمنی پایین برخی از این خودروها در مقابل سرقت، شرایط مناسبی را برای سارقین فراهم کرده تا با سود بیشتری به این عمل مجرمانه دست بزنند. این عوامل در مجموع منجر به افزایش آمار سرقت خودرو در سال‌های اخیر در مقایسه با گذشته شده است [۲].

در صنعت خودروسازی از فناوری‌های نوینی همچون سیستم‌های مانیتورینگ، الگوریتم ژنتیک [۳]، هوش مصنوعی، یادگیری عمیق [۴]، بینایی ماشین، آکوستیک امیشن [۵]، سیستم‌های احراز هویت بر اساس شاخص‌های بیومتریک [۶] و ... استفاده می‌شود. با این وجود، مطالعات نشان می‌دهد احتمال از دست دادن مالکیت وسایل نقلیه بر اثر سرقت، سه برابر بیشتر از سایر موارد است. آمارها حاکی از آن است که سالانه ده‌ها هزار خودرو در ایران به سرقت می‌رود و متوسط زمان لازم برای سرقت یک خودرو در ایران کمتر از ۲,۵ دقیقه است. بر اساس اطلاعات موجود در سال ۱۳۹۵، حدود ۴۰ درصد از کل سرقت‌های انجام‌شده مربوط به سرقت خودرو بوده است. سارقان معمولاً از روش‌های مختلفی برای سرقت خودرو استفاده می‌کنند. ساده‌ترین روش، شکستن شیشه یا باز کردن درب خودرو است. از دیگر روش‌های سرقت خودرو می‌توان به از کار انداختن دزدگیر اشاره کرد. اگرچه نیروهای امنیتی از شیوه‌های متنوعی برای تعقیب، ردیابی و توقف خودروهای سرقتی استفاده می‌کنند، اما پیشگیری از سرقت در مرحله اولیه رویکرد مؤثرتری محسوب می‌شود. محققین معدودی در زمینه‌ی بررسی سیستم‌های ایمنی و سرقت خودرو، تحقیق نموده‌اند که در ادامه به برخی از آن‌ها اشاره خواهد شد.

محمد اکمل بن عکاشه [۷] در سال ۲۰۰۶ سیستمی جهت استارت ماشین از راه دور طراحی کرد. وی در این پروژه از میکروکنترلر PIC16F84 استفاده نمود. استفان تیلیچ و مارسین وویجیک [۸] در سال ۲۰۱۲ به تجزیه‌وتحلیل امنیتی پروتکل ایموبیلایزر یک خودرو پرداخته و تعدادی از آسیب‌پذیری‌های امنیتی آن را کشف کردند. مادیلتی و همکاران [۹] در سال ۲۰۱۹ اقدام به طراحی سیستم کنترل خودرو با صدا نمودند. آن‌ها از برد آردوینو و ماژول بلوتوث برای این منظور استفاده کردند. در این پژوهش از دستورات صوتی ساده مانند چپ، راست، جلو، عقب، توقف برای اجرا استفاده شد. این دستورات از طریق یک اپلیکیشن اندرویدی به ماژول بلوتوث ارسال می‌شود. ریتیکا پاهوجا و نارندر کومار [۱۰] موفق به طراحی و ساخت خودروی رباتیک مبتنی بر پلتفرم آردوینو شدند که از طریق سیستم‌عامل اندروید کنترل می‌گردید. این سیستم با فعال‌سازی برنامه اندروید، یک رابط بصری در اختیار کاربر قرار می‌داد و اتصال بلوتوث را برقرار می‌نمود. ویجایان و همکاران [۱۱] موفق به طراحی و پیاده‌سازی یک سیستم امنیتی پیشرفته ضد سرقت خودرو شدند که از ترکیب احراز هویت اثرانگشت و رمز عبور بهره می‌برد. در این سیستم، کاربران ملزم به اسکن اثرانگشت خود هستند که پس از آن، سیستم به‌صورت خودکار هویت فرد را بررسی و تنها به کاربران مجاز اجازه راه‌اندازی موتور را می‌دهد. پیاده‌سازی این سامانه با استفاده از میکروکنترلر آردوینو MEGA انجام شده است. این راهکار هوشمند نه‌تنها فرآیند استارت خودرو را کاملاً خودکار نموده، بلکه با تلفیق فناوری تشخیص اثرانگشت و نظارت تصویری از طریق دوربین وب، سطح امنیتی قابل‌توجهی را فراهم می‌آورد. شاشیدهار و همکاران [۱۲] یک سیستم امنیتی مبتنی بر اثرانگشت برای جلوگیری از سرقت وسایل نقلیه

موتوری طراحی نمودند. در این سیستم که بر پایه برد آردوینو برنامه‌نویسی شده است، از یک حسگر اثرانگشت برای احراز هویت کاربران مجاز استفاده می‌شود. اگر داده‌های حسگر و داده‌های ذخیره‌شده در پایگاه داده هر دو مطابقت داشته باشند، وسیله نقلیه روشن خواهد شد؛ در غیر این صورت موقعیت مکانی خودرو به کمک GPS به مالک خودرو SMS می‌گردد و او را از تلاش غیرمجاز برای دسترسی مطلع می‌سازد. ردی و همکاران [۱۳] یک سیستم امنیتی مبتنی بر بیومتریک برای جلوگیری از سرقت خودرو توسعه دادند. در این سیستم که بر پایه‌ی پلتفرم آردوینو پیاده‌سازی شده، از فناوری تشخیص اثرانگشت به‌عنوان لایه اول امنیتی استفاده می‌شود. فرآیند کار سیستم به این صورت است که ابتدا مالک می‌بایست اثرانگشت خود را در سیستم ثبت و ضبط نماید. سپس در هنگام استفاده، حسگر اثرانگشت، الگوی بیومتریک کاربر را اسکن کرده و با نمونه‌های ثبت‌شده در پایگاه داده محلی مقایسه می‌کند. در صورت تطابق، سیستم یک درخواست تأیید دومرحله‌ای از طریق SMS برای مالک ارسال می‌نماید. اگر مالک درخواست را از طریق تلفن همراه خود بپذیرد، وسیله نقلیه روشن خواهد شد. آراویند و همکاران [۱۴] موفق به طراحی و ساخت یک سیستم ایمنی ضد سرقت خودرو شدند. آن‌ها برای روشن کردن موتور از فناوری تشخیص اثرانگشت و برای برنامه‌نویسی از میکروکنترلر آردوینو استفاده نمودند. به‌منظور افزایش ضریب امنیتی و امکان ردیابی، این سیستم مجهز به ماژول GPS برای تعیین موقعیت مکانی و ماژول GSM برای ارتباطات از راه دور می‌باشد. پاتیل و همکاران [۱۵] موفق به طراحی و ساخت یک سیستم هوشمند ضد سرقت مبتنی بر اینترنت اشیا (IoT) شدند. واحد سخت‌افزاری این سیستم شامل اجزای کلیدی مانند میکروکنترلرهای ESP8266 و ESP32-CAM، سنسور PIR، نمایشگر LCD، آلارم صوتی، LED و LDR است. سیستم مذکور در دو حالت روز و شب عمل می‌کند و از تشخیص چهره در حالت روز برای احراز هویت کاربران مجاز و از تشخیص حرکت به کمک سنسور حرکتی PIR در حالت شب برای تشخیص تهدید استفاده می‌نماید. پس از شناسایی فعالیت مشکوک، سیستم اعلان‌های هشدار را از طریق شبکه‌های مجازی مانند Telegram فعال می‌کند و نسبت به ارسال مستندات موجود سریعاً اقدام می‌نماید.

برای ارتقای امنیت خودرو و پیشگیری از سرقت، راهکارهای متنوعی مورد استفاده قرار می‌گیرد. هرچند که همه‌ی این راهکارها، ایمنی کامل خودرو را تضمین نمی‌کنند ولی می‌توانند، برحسب نوع طرح و مکانیزمی که دارند، به‌عنوان عامل بازدارنده‌ی سرقت در خودرو مورد استفاده قرار گیرند. تعدادی از طرح‌ها به شرح ذیل می‌باشد [۱۶، ۱۷، ۱۸]:

- سیستم‌های ضد سرقت مکانیکی مانند قفل فرمان، قفل پدال، قفل ترمزدستی و قفل چرخ‌ها
- سیستم سوئیچ مخفی که در خودروهای قدیمی جریان برق کویل به دلکو را قطع می‌نماید.
- سیستم‌های ضد سرقت الکترونیکی شامل انواع دزدگیرها و سیستم‌های هشداردهنده
- سیستم ایموبیلایزر که از اواسط دهه ۱۹۹۰ به‌منظور کاهش تعداد سرقت‌های خودرو توسعه داده شد.

هدف از این پژوهش بررسی و ارائه راهکارهای نوین برای پیشگیری از سرقت خودروها با استفاده از فناوری‌های پیشرفته است. در این سیستم برای جلوگیری از سرقت از سه لایه امنیتی، احراز هویت بیومتریک (اثرانگشت)، تکنولوژی RFID و صفحه‌کلید جهت ورود کد امنیتی به‌صورت هم‌زمان استفاده شده است. نوآوری اصلی این تحقیق در ارائه یک معماری امنیتی ترکیبی است که با تحلیل نقاط ضعف سیستم‌های موجود و ادغام هوشمندانه این سه لایه امنیتی، میزان موفقیت در پیشگیری از سرقت را به‌طور چشمگیری افزایش داده و آسیب‌پذیری‌های خودروها را کاهش می‌دهد. نتایج آزمایش‌های میدانی نشان می‌دهد که این راهکار می‌تواند ارتقاء سطح امنیت خودروها را به دنبال داشته باشد و سطح جدیدی از امنیت و آسایش خاطر را برای مالکان وسایل نقلیه به ارمغان آورد.

طراحی سیستم و نحوه اجرا

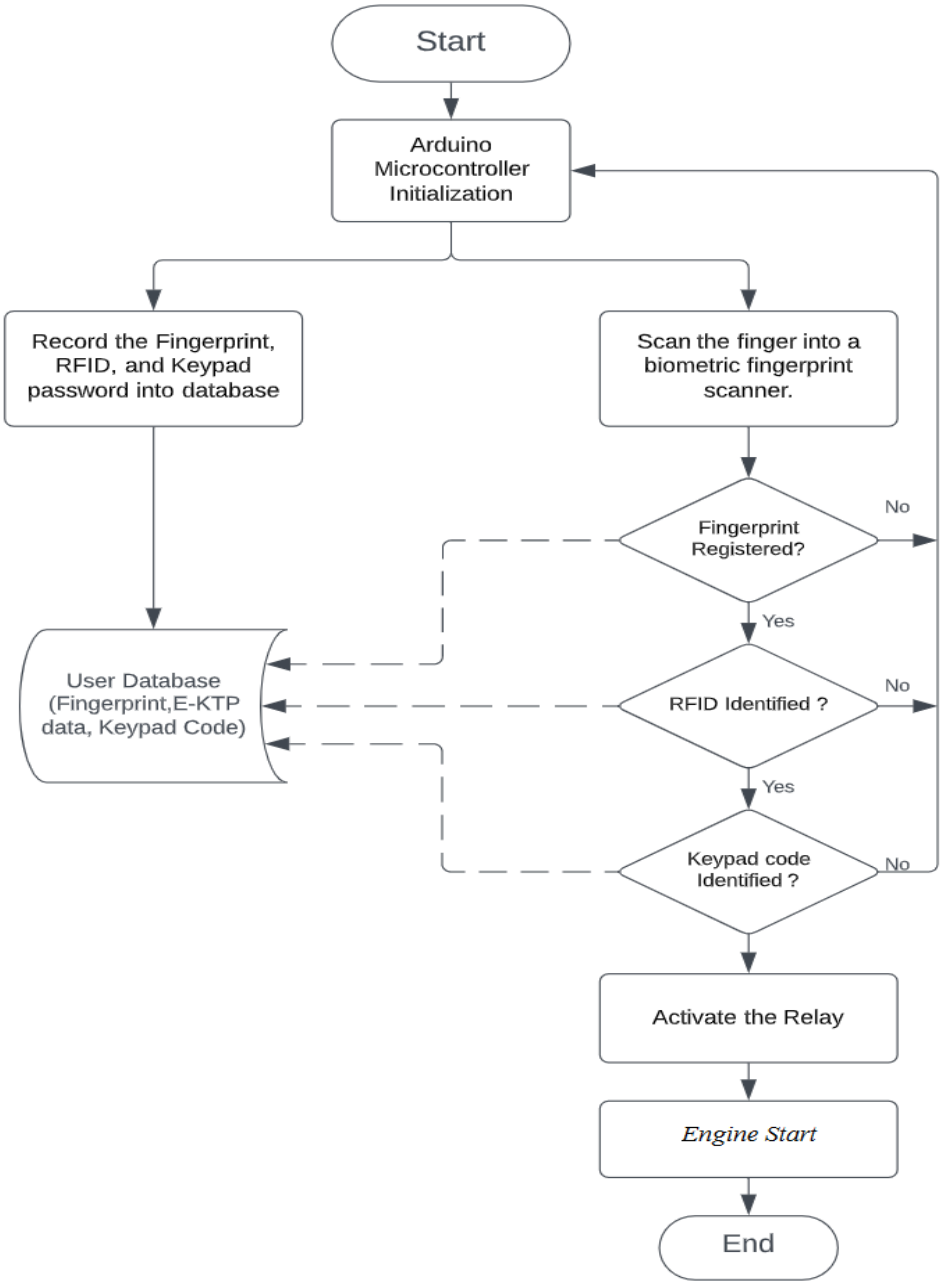
در این پژوهش یک سیستم امنیتی سه لایه طراحی و نمونه اولیه آن ساخته شد. سیستم مذکور از سه روش احراز هویت ترکیبی بهره می‌برد: ۱) شناسایی بیومتریک از طریق اثرانگشت، ۲) تکنولوژیRFID و ۳) ورود کد امنیتی از طریق صفحه‌کلید. در این مدار الکترونیکی می‌توان فعال شدن سوئیچ، بیدار شدن ECU، کار کردن پمپ‌بنزین و همچنین شروع جرقه‌زنی را منوط به دریافت این اطلاعات نمود و تا زمانی که اطلاعات صحیح از سه لایه امنیتی دریافت نشود، از فعال شدن سیستم جلوگیری کرد. برای کدنویسی سیستم از برد آردوینو استفاده شد. آردوینو، دارای یک نرم‌افزار متن باز اختصاصی برای برنامه‌نویسی بردهای خود می‌باشد که به نام نرم‌افزار آردوینو IDE (محیط توسعه یکپارچه آردوینو) شناخته می‌شود و امکان برنامه‌نویسی میکروکنترلر را از طریق اتصال مستقیم درگاه USB و بدون نیاز به پروگرامر خارجی فراهم می‌سازد [۱۹، ۲۰].

در این سیستم، ابتدا پایگاه داده‌ای حاوی اطلاعات بیومتریک اثرانگشت کاربر، کارت‌های هویتی RFID و رمز صفحه‌کلید ایجاد می‌شود که به‌عنوان مرجع اصلی فرآیند احراز هویت عمل می‌کند. برای روشن کردن موتور، کاربر ابتدا انگشت خود را روی اسکنر اثرانگشت قرار می‌دهد که پس از شناسایی اولیه، پردازش داده‌ها توسط برد آردوینو انجام شده و با تولید یک سیگنال ولتاژ، صحت اثرانگشت تأیید یا رد می‌شود. در صورت تطابق، سیستم به مرحله بعدی یعنی اسکن کارت RFID توسط ماژول کدخوان می‌رود و پس از تأیید این مرحله، کاربر باید کد امنیتی از پیش تعیین‌شده را از طریق صفحه‌کلید عددی وارد نماید. در نهایت، اگر هر سه مرحله احراز هویت با موفقیت طی شود، یک رله به‌عنوان سوئیچ دیجیتال عمل می‌کند و رله فعال شده و موتور روشن می‌شود. این معماری سه‌لایه، امنیت سیستم را به‌طور تصاعدی افزایش خواهد داد و فلوچارت آن در شکل ۱ قابل مشاهده است.

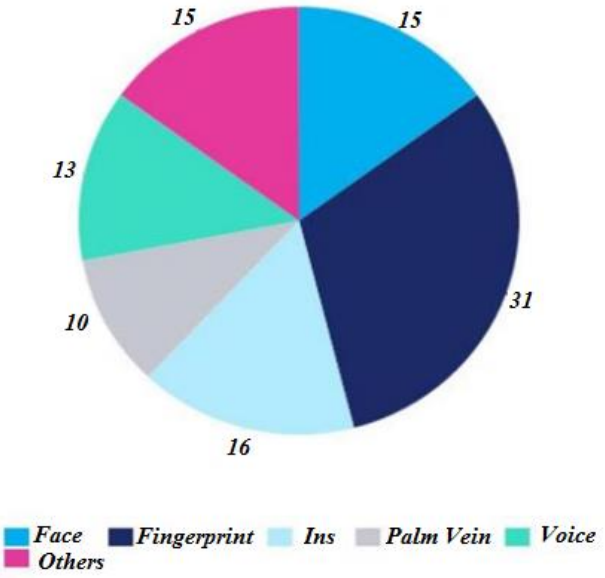
مکانیزم احراز هویت با استفاده از حسگر اثرانگشت

سیستم‌های شناسایی بیومتریک از جمله روش‌های نوین امنیتی محسوب می‌شوند که با استفاده از ویژگی‌های فیزیولوژیکی و رفتاری منحصربه‌فرد افراد، امکان شناسایی و احراز هویت را فراهم می‌کنند [۲۱، ۲۲]. استفاده از این سیستم‌ها برای شناسایی یا راستی‌آزمایی روزبه‌روز در حال افزایش است، زیرا تکرار کیفیت‌های بیومتریک بسیار دشوار است و برای تمام عمر تغییر نمی‌کنند [۲۳]. در این میان، تشخیص اثرانگشت به دلیل دقت بالا و منحصربه‌فرد بودن الگو برای هر فرد، یکی از پرکاربردترین روش‌های بیومتریک به‌عنوان یک سیستم امنیتی بسیار ایمن است. اگرچه روش‌های دیگری مانند تشخیص صدا، تشخیص چهره، اسکن عنبیه و تشخیص الگوی ورید کف دست نیز وجود دارند [۲۴، ۲۵]. همان‌طور که در شکل ۲ مشاهده می‌شود، سیستم تشخیص اثرانگشت به‌عنوان مؤثرترین و پراستفاده‌ترین روش بیومتریک در سیستم‌های امنیتی شناخته می‌شود که این امر ناشی از ترکیب دقت بالا، سهولت استفاده و مقرون‌به‌صرفه بودن است.

در جدول ۱ تفاوت روش‌های مختلف بیومتریک نشان داده شده است.



شکل ۱. فلوچارت برنامه نوشته‌شده



شکل ۲. درصد بیومتریک استفاده‌شده در سیستم‌های امنیتی [۲۶]

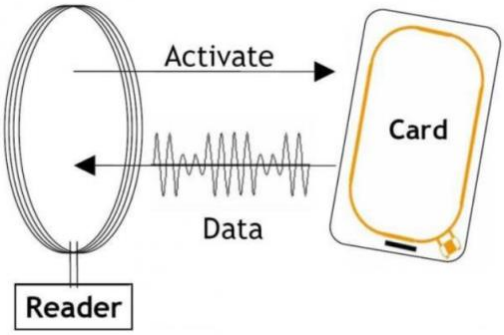
جدول ۱. تفاوت روش‌های بیومتریک [۲۶]

روش بیومتریک	دقت	آسان برای استفاده	پذیرش کاربر
تشخیص چهره	کم	بالا	بالا
تشخیص اثرانگشت	بالا	متوسط	کم
اسکن عنبیه	بالا	متوسط	متوسط
تشخیص الگوی ورید کف دست	بالا	بالا	متوسط
تشخیص صدا	متوسط	بالا	بالا

مکانیزم احراز هویت با استفاده از کارت RFID

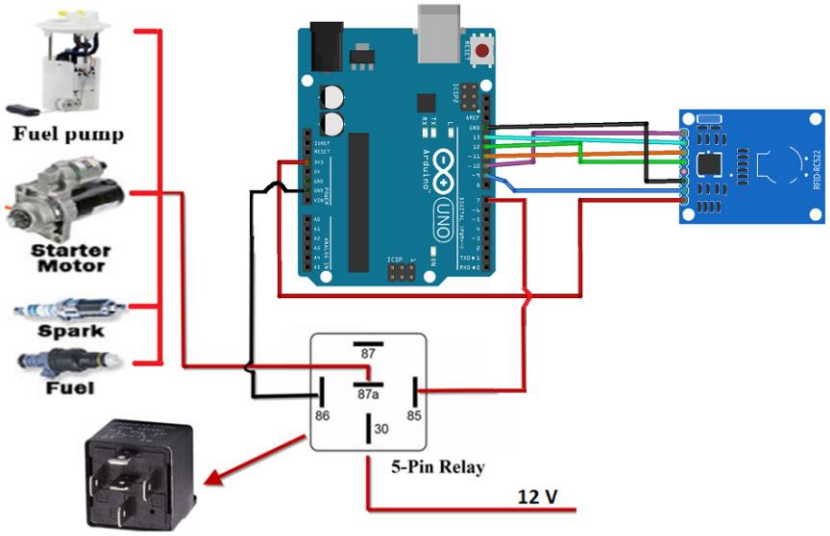
RFID (شناسایی با فرکانس رادیویی[۱]) یک سیستم شناسایی بی‌سیم با امواج رادیویی است که از سه بخش اصلی چیپ (تگ)، آنتن و کدخوان تشکیل شده است. تگ یا برچسب هوشمند، دستگاه فرستنده خودکار شامل یک مدار الکترونیکی است که به شیء موردنظر که لازم است دارای یک کد شناسایی باشد، متصل می‌گردد. هنگامی‌که تگ به محدوده کدخوان نزدیک می‌شود، میدان مغناطیسی ایجادشده توسط کدخوان، تگ را فعال می‌کند و تگ به ارسال پیوسته داده‌ها از طریق پالس‌های رادیویی می‌پردازد. در نهایت داده‌ها توسط کدخوان دریافت و توسط نرم‌افزارهای مربوطه پردازش می‌گردد. RFID همچنین باید دارای پایگاه داده‌ای باشد که اطلاعات مربوط به هر شیء که تگ بر روی آن نصب شده را در داخل خود ذخیره کند. شماتیک عملکرد RFID در شکل ۳ نمایش داده شده است.

[۱] Radio Frequency Identification



شکل ۳. شماتیک عملکرد RFID

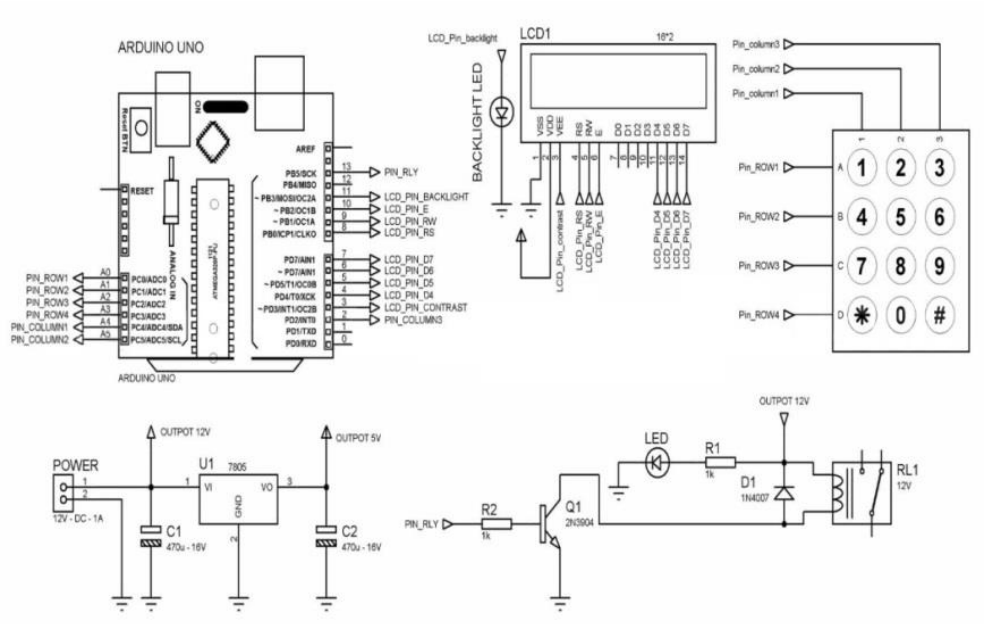
در پژوهش حاضر از ماژول RFID Reader RC522 استفاده شده است. این ماژول یک میدان الکترومغناطیسی ۱۳،۵۶ مگاهرتز تولید می‌کند که برای ارتباط با برچسب RFID استفاده می‌شود. در شکل ۴ نحوه اتصال این ماژول به برد آردوینو نمایش داده شده است. در این سیستم، در صورت تطابق اطلاعات کارت RFID با داده‌های ثبت‌شده، پایه ۷ آردوینو فعال می‌شود و سیگنال فعال‌سازی را به پایه ۸۵ رله ارسال می‌کند. رله که از طریق پایه‌های ۸۵ و ۸۶ کنترل می‌شود، در حالت عادی (غیرفعال بودن) جریان ورودی پایه ۳۰ را به پایه ۸۷ هدایت می‌کند، اما پس از فعال‌شدن، مسیر جریان به پایه ۸۷a تغییر می‌یابد و برق را به پمپ‌بنزین، استارت، سیستم جرقه‌زنی و انژکتورها ارسال می‌نماید. لازم به ذکر است سیستم به‌گونه‌ای برنامه‌ریزی شده که در صورت فعال شدن رله، نهایتاً ۵ دقیقه زمان به‌منظور استارت زدن وجود دارد و پس از آن سیستم غیرفعال می‌شود و برای فعال شدن مجدد، نیاز به احراز هویت دوباره با کارت RFID دارد.



شکل ۴. استفاده از RFID Reader RC522 برای راه‌اندازی برد آردوینو

مکانیزم احراز هویت با استفاده از کد فعال‌سازی

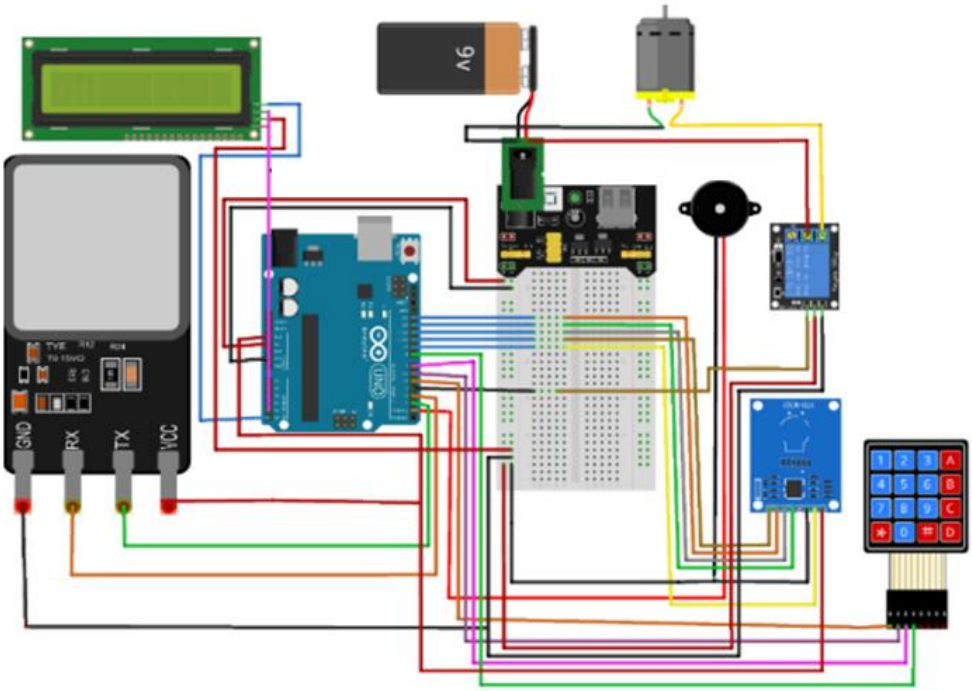
برای ورود کد فعال‌سازی به سیستم از یک کیپد استفاده شده است. بر اساس الگوریتم اولیه که برای برنامه‌نویسی در نظر گرفته شد، ابتدا کد توسط برنامه دریافت می‌شود و با کدی که از پیش در برنامه تعریف شده است، مقایسه می‌گردد. در صورت تطابق، سیستم اجازه فعال شدن پمپ‌بنزین، استارت، کویل دوبل و انژکتورها را صادر می‌کند. چنانچه کد واردشده نادرست باشد، سیستم درخواست واردکردن مجدد کد را ارائه می‌دهد. لازم به ذکر است درصورتی‌که کاربر سه بار متوالی کد اشتباه وارد نماید، سیستم به‌صورت خودکار بوق هشدار را به مدت ۲۰ ثانیه فعال می‌کند. نقشه شماتیک اتصال کیپد و LCD به برد آردوینو در شکل ۵ نشان داده شده است.



شکل ۵. نقشه شماتیک اتصال کیپد و LCD به برد آردوینو

نتایج و بحث

به‌منظور بررسی عملکرد سیستم، برد عملیاتی نهایی طراحی و پیاده‌سازی شد که در آن به‌جای پمپ‌بنزین، کویل دوبل، استارت و انژکتور از یک الکتروموتور به‌عنوان شاخص عملکرد استفاده گردید (شکل ۶). برد نهایی شامل سه ماژول اصلی احراز هویت (حسگر اثرانگشت، تراشه RFID و صفحه کیپد برای ورود رمز عبور) می‌باشد. ماژول RFID و حسگر اثرانگشت با ولتاژ ۳٫۳ ولت کار می‌کنند، درحالی‌که ماژول صفحه‌کلید، نمایشگر LCD ۲×۱۶، رابط I2C، Buzzer و کلیه رله‌ها به منبع تغذیه ۵ ولتی نیاز دارند. از سوی دیگر، الکتروموتور که به‌عنوان شبیه‌ساز سیستم خودرو عمل می‌کند، به ولتاژهای ۹ و ۱۲ ولت نیاز خواهد داشت. این معماری چندولتاژی به‌دقت برنامه‌ریزی شده تا تمامی اجزا به‌صورت هماهنگ و با حداکثر کارایی عمل نمایند.



شکل ۶. شماتیک کلی سیستم

به‌منظور بررسی مدت‌زمان لازم برای اسکن اثرانگشت، ده مرتبه اسکن اثرانگشت انجام گرفت و متوسط زمان پاسخ سیستم ثبت شد. جدول ۲ مقادیر مدت‌زمان لازم برای اسکن اثرانگشت را برای هر آزمایش نشان می‌دهد. نتایج نشان داد متوسط زمان لازم برای اسکن اثرانگشت ۳٫۷ ثانیه می‌باشد.

جدول ۲. مدت‌زمان لازم برای اسکن اثرانگشت

آزمایش	زمان (S)
۱	۳٫۶
۲	۳٫۸
۳	۳٫۵
۴	۳٫۷
۵	۳٫۹
۶	۳٫۸
۷	۳٫۷
۸	۳٫۶
۹	۳٫۹
۱۰	۳٫۵
متوسط	۳٫۷

همچنین به‌منظور بررسی مدت‌زمان لازم برای اسکن کارت RFID از ده کارت با IDهای مختلف استفاده شد و متوسط زمان پاسخ سیستم به دست آمد. نتایج نشان داد متوسط زمان لازم برای اسکن کارت RFID تقریباً ۲,۴ ثانیه است. مدت‌زمان لازم برای اسکن کارت RFID با ID کارت‌های مختلف در جدول ۳ گزارش شده است.

جدول ۳. مدت‌زمان لازم برای اسکن کارت RFID (با ID کارت‌های مختلف)

آزمایش	زمان (S)
۱	۲
۲	۲,۲
۳	۲,۵
۴	۲,۱
۵	۲,۲
۶	۲,۶
۷	۲,۴
۸	۲,۹
۹	۲,۴
۱۰	۲,۷
متوسط	۲,۴

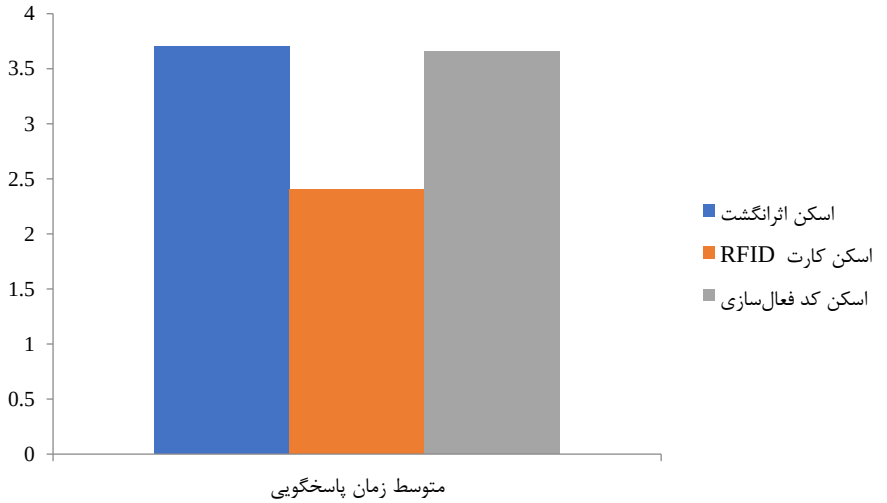
در نهایت به‌منظور بررسی مدت‌زمان لازم برای تحلیل کد فعال‌سازی واردشده، ده مرتبه کد فعال‌سازی وارد گردید و متوسط زمان پاسخ سیستم ثبت شد. جدول ۴ مقادیر مدت‌زمان لازم برای اسکن کد فعال‌سازی را برای هر آزمایش نشان می‌دهد. نتایج نشان داد متوسط زمان لازم برای تحلیل کد فعال‌سازی تقریباً ۳,۶۶ ثانیه است.

جدول ۴. مدت‌زمان لازم برای اسکن کد فعال‌سازی

آزمایش	زمان (S)
۱	۳,۶
۲	۳,۸
۳	۳,۵
۴	۳,۷
۵	۳,۹
۶	۳,۵
۷	۳,۷
۸	۳,۸
۹	۳,۵
۱۰	۳,۶
متوسط	۳,۶۶

نتایج آزمایش‌های انجام‌شده نشان می‌دهد سیستم امنیتی سه‌لایه طراحی‌شده با ترکیب روش‌های احراز هویت اثرانگشت، تکنولوژی RFID و کیپد، عملکرد مؤثری در جلوگیری از سرقت خودرو دارد. میانگین زمان پاسخگویی سیستم برای اسکن اثرانگشت ۳,۷ ثانیه، برای خواندن کارت‌های RFID 2.4 ثانیه و برای تحلیل کد فعال‌سازی ۳,۶۶ ثانیه اندازه‌گیری شد که در مجموع زمان کل احراز هویت را به ۹,۷۶ ثانیه می‌رساند. این مقادیر در جداول ۲ تا ۴ به تفصیل ارائه شده‌اند.

همان‌طور که در شکل ۷ مشاهده می‌شود، لایه RFID با ۲,۴ ثانیه سریع‌ترین و اسکن اثرانگشت با ۳,۷ ثانیه کندترین زمان پاسخ را دارند. نکته قابل توجه، پایداری سیستم در تمامی آزمایش‌ها است که دامنه تغییرات زمانی در هر لایه کمتر از ۰,۵ ثانیه بوده است. نتایج ارزیابی زمان پاسخگویی سیستم احراز هویت سه‌لایه نشان‌دهنده عملکرد بهینه آن است و نشان می‌دهد سیستم طراحی‌شده ضمن حفظ دقت و امنیت بالا، از سرعت پاسخگویی مناسبی برای کاربردهای عملی برخوردار است. مقایسه این زمان‌ها با استانداردهای صنعتی نشان می‌دهد سیستم حاضر در محدوده قابل قبولی قرار دارد و می‌تواند به عنوان یک راه‌حل امنیتی مؤثر در خودروها مورد استفاده قرار گیرد.



شکل ۷. متوسط زمان لازم برای پاسخگویی هر یک از مکانیزم‌های احراز هویت

همچنین نتایج ارزیابی عملی سیستم بر روی موتور چهار سیلندر خطی، نشان‌دهنده عملکرد مؤثر آن در جلوگیری از استارت غیرمجاز است. در این آزمایش‌ها که پس از نصب کامل اتصالات برد الکترونیکی انجام شد، سیستم به‌درستی از فعال شدن موتور در مواردی که احراز هویت به‌طور کامل انجام نشده بود، ممانعت به عمل آورد. این تست‌های عملیاتی، اثربخشی سیستم سه‌لایه امنیتی طراحی‌شده (شامل اثرانگشت، RFID و کد عددی) را در شرایط واقعی به‌خوبی تأیید می‌نماید و نشان می‌دهد که راهکار پیاده‌سازی‌شده قادر است امنیت موتور را در برابر سرقت به میزان قابل‌توجهی افزایش دهد. عملکرد بدون نقص سیستم در تمامی سناریوهای آزمایشی، قابلیت اطمینان بالای این طراحی را به نمایش می‌گذارد.

نتیجه‌گیری

امنیت خودروها همواره دغدغه‌ای اساسی برای مالکان بوده است. با پیشرفت فناوری و پیچیده‌تر شدن روش‌های سرقت، ضرورت ارتقای سیستم‌های امنیتی خودروها بیش‌ازپیش احساس می‌شود. سارقین همواره در کمین هستند تا از کوچک‌ترین ضعف امنیتی در خودروها استفاده کنند و اقدام به دستبرد نمایند. این پژوهش موفق به طراحی و ساخت یک سیستم چندلایه امنیتی ضد سرقت خودرو شد که ترکیبی هوشمندانه از فناوری‌های احراز هویت بیومتریک (اثرانگشت)، RFID و کد عددی را به کار می‌گیرد. به‌منظور برنامه‌نویسی از میکروکنترلر آردوینو استفاده شد. نتایج نشان داد که سیستم RFID با میانگین ۲٫۴ ثانیه سریع‌ترین روش و اسکن اثرانگشت با میانگین ۳٫۷ ثانیه کندترین روش در دریافت اطلاعات توسط برد آردوینو است. در مجموع سیستم سه لایه طراحی‌شده جهت فعال شدن نیاز به ۹٫۷۶ ثانیه زمان دارد. در این مدار الکترونیکی می‌توان فعال شدن سوئیچ، بیدار شدن ECU، کار کردن پمپ‌بنزین و همچنین شروع جرقه‌زنی را منوط به دریافت این اطلاعات نمود و تا زمانی که اطلاعات صحیح از سه لایه امنیتی دریافت نشود، از فعال شدن سیستم جلوگیری کرد. این سیستم بعد از طراحی بر روی یک موتور چهار سیلندر خطی نصب و آزمایش‌های میدانی متعددی در شرایط واقعی به‌منظور ارزیابی عملکرد آن انجام شد. نتایج این ارزیابی‌ها نشان داد که سیستم طراحی‌شده به‌طور کاملاً مؤثر از فعال شدن موتور در مواردی که احراز هویت به‌طور کامل انجام نشده باشد (شامل عدم تطابق اثرانگشت، استفاده از کارت RFID غیرمجاز یا واردکردن کد اشتباه) جلوگیری می‌کند. این راهکار نوین با ارائه سطح امنیتی چندلایه و زمان پاسخ‌دهی مناسب، گامی مؤثر در ارتقای امنیت خودروها و کاهش نگرانی‌های مالکان محسوب می‌شود و پتانسیل بالایی برای کاربرد در صنعت خودروسازی دارد.

References

[1] Khodae, A. (2023). The identification of male stolen vehicles using car tracking technique. *karagah*, *17*(64), 7-35. [In Persian]. https://doi.org/10.22034/det.2023.1271507.1365

[2] Kohandani, B. (2020). Preparing Competence-based CID Police Agents in Detecting Stolen Vehicles. *karagah*, *14*(50), 112-127. [In Persian]. https://doi.org/10.22034/det.2020.94642

[3] Rahmatinejad, B., Abbasgholipour, M., & Mohammadi Alasti, B. (2021). Redesign of engine radiator based on number of optimal fans using a genetic algorithm. *Karafan Quarterly Scientific Journal*, *17*(4), 99-118. [In Persian]. https://doi.org/10.48301/kssa.2021.128398

[4] Taghandiki, K., Dallakehnejad, M., & Rahimi Asiabaraki, H. (2024). Reducing Air Pressure System Repair Costs in Scania Trucks through Deep Learning. *Journal of Engineering and Applied Research*, *1*(1), 183-196. https://doi.org/10.48301/JEAR.2024.447671.1022

[5] Rahmatinejad, B., Rahimi Asiabaraki, H., & Azimpour Shishevan, F. (2023). Diagnosing Dimensional Defects and Valve Cracks Using Machine Vision and Acoustic Emission. *Karafan Journal*, *20*(3), 149-168. [In Persian]. https://doi.org/10.48301/kssa.2023.391572.2501

[6] Motamedi, M. (2024). Designing a Fuzzy Expert System to Investigate the Impact of Biometric Indicators and Radio Waves on Authentication. *Karafan Journal*, *21*(3), 85-110. [In Persian]. https://doi.org/10.48301/kssa.2024.445634.2848

[7] Akashah, M. A. (2006). *Remote Control Car Starter (RCCS)* (Doctoral dissertation, KUKTEM). https://core.ac.uk/download/pdf/159177213.pdf

[8] Tillich, S., & Wójcik, M. (2012). Security analysis of an open car immobilizer protocol stack. In *Trusted Systems: 4th International Conference, INTRUST 2012, London, UK, December 17-18, 2012. Proceedings 4* (83-94). Springer Berlin Heidelberg. https://doi.org/10.1007/978-3-642-35371-0_8

[9] Maddileti, T., Jammigumpula, M., Jagadish Kumar, H., & Sai Sashank, K. V. (2019). Voice controlled car using Aurduino and Bluetooth module. *Int J Eng Adv Technol IJEAT*, ۹(۲), ۱۰۶۲-۱۰۶۵. https://doi.org/10.35940/ijeat.B3673.129219

[10] Pahuja, R., & Kumar, N. (2014). Android mobile phone controlled bluetooth robot using 8051 microcontroller. *International Journal of Scientific Engineering and Research*, ۲(۷), ۱۴-۱۷. https://www.ijser.in/v2i7.php

[11] Vijayan, P. M., Vandana, P., Yogeswar, M., Kumar, S. S., Vijayalakshmi, A., & Vishnu, R. (2024, May). Advanced Fingerprint And Passcode Based Anti-Theft Vehicle System. In *2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT)* (1-6). IEEE. https://doi.org/10.1109/AIIoT58432.2024.10574591

[12] Shashidhar, K., kumar Dharmireddy, A., & Rao, C. M. (2024). Anti-Theft Fingerprint Security System for Motor Vehicles. In *Blockchain Technology for IoT and Wireless Communications* (89-101). CRC Press. https://www.taylorfrancis.com/chapters/edit/10.1201/9781003269991-8/anti-theft-fingerprint-security-system-motor-vehicles-shashidhar-ajay-kumar-dharmireddy-ch-madhava-rao

[13] Reddy, K. H., Sunchu, P., Bojja, A. R., & Rallapalli, P. V. (2024, February). Implementation of anti-theft security alarm system for vehicles. In *AIP Conference Proceedings* (2942,1). AIP Publishing. https://doi.org/10.1063/5.0196547

[14] Aravind, M. N., Ranadheer, R., Navya, P., Kiran, M. U., & Reddy, S. S. (2024). Fingerprint based vehicle anti-theft security system and vehicle ignition with location tracking. *International Journal of Engineering Research and Science & Technology*, ۲۰(۲), ۹۵-۱۰۲. https://ijerst.org/index.php/ijerst/article/view/262

[15] Patil, M. N., Hattaraki, S. M., Ukkali, P. S., Rathod, P. B., Shatgar, D. D., & Metri, P. B. (2024, September). Smart Anti-Theft Control System Using IoT. In *2024 IEEE North Karnataka Subsection Flagship International Conference (NKCon)* (1-5). IEEE. https://doi.org/10.1109/NKCon62728.2024.10774803

[16] Rahimi Asiabaraki, H. (2018). *Design and construction of the CIM Immobilizer training set*. Technical and Vocational University (TVU). [In Persian]

[17] Rahmatinejad, B., Rahimi Asiabaraki, H., & Ghasemi Zavaregh, H. (2019). *Design and construction of the Bosch Immobilizer training set*. Technical and Vocational University (TVU). [In Persian]

[18] Ghanbari, M., & Rahimi Asiabaraki, H. (2020). *Design and construction of the SSAT Immobilizer training set*. Technical and Vocational University (TVU). [In Persian]

[19] Marhoon, H. M., & Taha, I. A. (2018). Design and implementation of intelligent circuit breaker for electrical current sensing and monitoring. *International Journal of Core Engineering & Management (IJCEM), 11*(4), 39-50. https://www.researchgate.net/publication/324507273_DESIGN_AND_IMPLEMENTATION-OF-INTELLIGENT-CIRCUIT-BREAKER-FOR-ELECTRICAL-CURRENT-SENSING-AND-MONITORING

[20] Badamasi, Y. A. (2014, September). The working principle of an Arduino. In *2014 11th international conference on electronics, computer and computation (ICECCO)* (1-4). IEEE. https://doi.org/10.1109/ICECCO.2014.6997578

[21]Lourde, M., & Khosla, D. (2010). Fingerprint identification in biometric securitysystems. *International Journal of Computer and Electrical Engineering*, *2*(5), 852. https://doi.org/10.7763/IJCEE.2010.V2.239

[22] Ali, M. M., Mahale, V. H., Yannawar, P., & Gaikwad, A. T. (2016, March). Overview of fingerprint recognition system. In *2016 international conference on electrical, electronics, and optimization techniques (ICEEOT)* (1334-1338). IEEE. https://doi.org/10.1109/ICEEOT.2016.7754900

[23] Ross, A., Nandakumar, K., & Jain, A. K. (2008). Introduction to multibiometrics. *Handbook of biometrics*, 271-292. https://doi.org/10.1007/978-0-387-71041-9_14

[24] Kiruthiga, N., & Latha, L. (2014). A study of biometric approach for vehicle security system using fingerprint recognition. *International Journal of Advanced Research Trends in Engineering and Technology (IJARTET), 1*(2). https://ijartet.com/Vol-one-issue-two

[25] Priyanka. (2014, August). Fingerprint recognition techniques and its applications. In *2014 International Conference on Advances in Engineering & Technology Research (ICAETR-2014)* (1-6). IEEE. https://doi.org/10.1109/ICAETR.2014.7012906

[26] Rivandi, P., Winda, A., Satrio, D., & Solihin, M. I. (2019). Automotive start–stop engine based on fingerprint recognition system. In *E3S web of conferences* (130, 01022). EDP Sciences. https://doi.org/10.1051/e3sconf/201913001022