JCBI
Journal of Computing & Biomedical Informatics Volume 04 Issue 01
ISSN: 2710 - 1606 2022

*Research Article*
https://doi.org/10.56979/401/2022/114

# Cost Efficient Automobile Security Using Face Recognition and GSM Module

**Kanza Gulzar[1,*], Nauman Qadeer[2], Muhammad Aamir[3], Asif Nawaz[4], Hana Mujlid[5], Syed Muhammad Mohsin[6,7], Sheeraz Ahmed[8]**

[1]University Institute of Information Technology, PMAS Arid Agriculture University, Rawalpindi 46300, Pakistan.
[2]Department of Computer Science, Fedral Urdu University of Arts, Science and Technology, Islamabad, Pakistan.
[3]College of Computer Science, Sichuan University Chengdu, China.
[3]College of Computer Science, Huanggang Normal University, Huanggang, China
[4]Higher Colleges of Technology, Dubai, U.A.E.
[5]Department of Computer Engineering, Taif University, Taif, Saudi Arabia.
[6]Department of Computer Science, COMSATS University Islamabad, Islamabad 45550, Pakistan.
[7]College of Intellectual Novitiates (COIN), Virtual University of Pakistan, Lahore 55150, Pakistan.
[8]Iqra National University, Peshawar, Pakistan.
[*]Corresponding Author: Kanza Gulzar. Email: kanza@uaar.edu.pk.

**Received:** September 01, 2022 **Accepted:** November 15, 2022 **Published:** December 29, 2022.

**Abstract:** Face detection is one of the most important modern computer vision topics. The importance of face recognition (FR) is increasing in our society for identification purposes. In this paper, we practically demonstrated the authenticity of an automatic security system for automobiles using face recognition technology. Our proposed system is not only a facial recognition system, but also supports authentication via a GSM module for remote monitoring and permission/control by a specific remote security code. The system was implemented and tested using a Raspberry Pi 3 board, Python and OpenCV to program the different modules for face recognition. The implementation results confirm the applicability of the proposed system as it offers the advantages of robustness, high accuracy, reliability and security at the lowest cost. This paper defines a combination of fail-safe algorithms for the GPS/GSM module in addition to face recognition algorithms, which are more suitable in dynamic environments where high uncertainties are expected and require high accuracy and reasonable speed. In future, we aim to develop an intelligent smart home application to meet the upcoming needs.

**Keywords:** Automobile; Face Recognition; GPS/GSM module; RaspberryPi; OpenCV.

## 1. Introduction

A lot of research has been done to increase security in our daily lives to ensure that we are safe. But research is also being done to eliminate that level of security. Automation has indeed had a positive impact, but there are numerous gaps in security systems to accomplish this task. The number of car thefts in Pakistan has increased over the past year. Between Jan. 1 and July 31, 2022, a total of 387 cars worth 580 million rupees were stolen in Rawalpindi district, a city adjacent to the federal capital. When a police officer in charge was questioned by Dawn, a leading English newspaper, he said that although these criminals are caught and brought to justice, they have to be released due to lack of evidence. He said, "We are really helpless because we have no strategy and no measures to catch these thieves due to lack of any evidence". To deal with this problem, a security system is needed that specifies exactly who has access to the car and who does not. For security and privacy reasons, various methods such as passwords and biometrics are used. Face recognition (FR) is not new, but it is getting better every day [2]. Other biometrics are also used

for security purposes, but until now, FR recognition is still one of the most studied topics in biometrics [3,4,5].

The natural functioning of FR systems makes them the most popular biometric technique after fingerprints [6,7]. However, fingerprints have some weaknesses, e.g., access to the car is denied if the owner's fingers are injured. Therefore, FR is gradually becoming the most satisfactory and secure solution because it is impractical to embezzle a face and steal it on the spot to gain control of a car. Research continues to bring the technology of FR closer to the human level to develop robust security systems [8,9]. Some of these systems are already helping many people to secure their cars. However, these trackers are either too complex or too expensive to afford. Therefore, a user-friendly, low-cost, and robust approach is needed to reduce the risk of theft.

In our pilot study [10], we used the Arduino Uno to develop a low-cost car security system, but it has some limitations: (1) the Arduino does not have its own operating system, the microcontroller cannot run artificial intelligence (AI) algorithms at high speed, so we had to use it with a Windows or Mac operating system and a computer stick; (2) it does not provide remote access and does not inform the car owner about the car's location. When the owner is absent, such as when he needs to provide access to a family member or friend in his absence, the other person needs to train the system, which takes a little more time. On the other hand, a layperson cannot train the system. To overcome these limitations and improve the functionality of our project, we address these issues as follows: The Arduino is replaced by a Raspberry Pi module, a GSM module is added as it enables remote authentication and notifies the owner via SMS when an unauthorized person tries to enter the vehicle. OpenCV and principal component analysis (PCA) are used in the backend as their robust features are discussed in the side sections.

The rest of the paper consists of the section 2, which discusses the importance of the OpenCV based FR technique in light of the literature discussed. Section 3 explains the proposed system in terms of components and hardware implementation. Section 4 describes the software implementation and the results obtained with the proposed system. Section 5 provides a comparative analysis of the proposed system with the existing approaches in the literature and the automotive industry. Finally, Section 6 concludes the paper.

**2. Review of OpenCV based FR techniques**

As stated in the section above, due to the high rate of theft in everyday life, there is an increasing demand for a somewhat simpler technique to identify the perpetrators and ensure security. Consequently, FR is becoming an increasingly important aspect of computer vision in the development of security applications. We are trying to solve the security problem with low-cost components and simple coding techniques. Thus, OpenCV has been presented as a key to the problems of computer vision for improved detection and enhanced security measures [11]. The Haar cascade proposed by Viola Jones is a single method for object recognition. A machine learning method is developed for graphical recognition of an object, which enables fast image processing with high recognition rate [12].

The most commonly used algorithm for face recognition is PCA. There are many limitations in the implementation of PCA due to the high computational load. To deal with this problem, a method called frequency sub-bands has been proposed for applying PCA to specific wavelet sub-bands. Normally, PCA is applied to images of the entire human face, but Feng introduced the wavelet transform by decomposing the face images into frequency sub-bands. This is referred to as the usual demonstration of PCA. A comparative analysis of this approach with the previously used PCA showed that this approach is much better in recognition and reduces the computational cost [13].

Another commonly used detection technique is linear discriminant analysis (LDA), also known as Fisher linear discriminant analysis (FLDA). It works like PCA but with a reduced number of computations and is able to classify data according to their differences [14]. Local binary pattern histogram (LBPH) is also a face recognition method. In this method, the features that are preprocessed for face recognition are removed from the face images by dividing an image into many small parts. PCA processes the face as a whole. Face recognition is interesting and complex due to the impact of evaluation in the recognition phase. LBPH analyzes the image quality and its operator helps to compose the LBP program into the histogram for histogram overlap [15].

In [16], the authors compared the mentioned face recognition methods to develop an auto-attendance system. They pointed out the problems they faced in detecting faces and using different methods for face detection. A tabular comparison of the methods described above is shown in Table 1. After reviewing the comparison of the FR techniques supported by OpenCV, we conclude that the overall performance of PCA is more promising than the others. Therefore, we chose the PCA algorithm for FR.

**Table 1.** WCAG conformance levels description

| | Factors | | PCA | LDA | LBPH |
|---|---|---|---|---|---|
| Recognition Rate | Light variance | Greater | Ok | Ok | Poor |
| | | Normal | Excellent | Good | Good |
| | | Lesser | Ok | Ok | Ok |
| | Pose Variance | Greater | Excellent | Ok | Poor |
| | | Lesser | Good | Good | Ok |
| | Distance Variance | Farther | Ok | Poor | Poor |
| | | Closer | Excellent | Good | Good |
| | Dataset size Variance | Greater | Ok | Good | Poor |
| | | Lesser | Excellent | Excellent | Excellent |

## 3. Proposed system model

The proposed system is implemented in two modules. One consists of hardware components and the hardware implementation, and the other consists of the software that implements the FR technique. Basically, FR includes three key points. First, the face data is collected, then the face features are extracted, and finally the features are matched for recognition. Since the focus of this work is to provide a low-cost and easy-to-implement security system, the proposed system is discussed with these aspects in mind in the following section.

### 3.1 System components and hardware implementation details of our proposed system model

To achieve an effective design approach and high accuracy, many researchers are working to improve security systems in terms of efficiency, trustworthiness, and robustness by using more efficient face detection and recognition algorithms. At the same time, it is necessary to study the dynamic properties of the tools used. For this reason, we have paid a great attention to this issue and have used the Raspberry Pi 3 model B. In addition to the Raspberry Pi, the proposed system consists of a USB camera, a GSM/GPS module with Python and a free API that is OpenCV. Fig. 1 shows the structure diagrams for the proposed system. In the experiments, we used Raspberry Pi Shields to connect the GSM/GPRS SIM900 to GPS modules. The provided Shields are stacked on top of each other to perform multiple tasks at once. The structural diagram of the proposed system model is shown in Fig. 1 and the development setup is shown in Fig. 2.

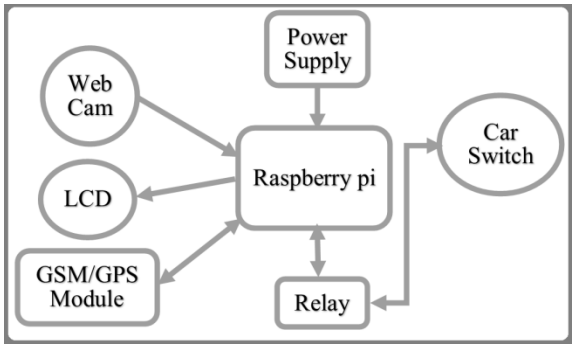



**Figure 1.** Structural diagram of the proposed system model

**Figure 2.** Development setup

3.1.2 Raspberry Pi

It is a tiny circuit board that functions as a computer (shown in Fig. 3), a system-on-chip (SoC), and a specially designed Linux operating system called Rasbian, the certified OS for Raspberry Pi. Other operating systems, such as Android, Firefox OS, RISC OS, Ubuntu Mate, etc., can also be used for the Raspberry Pi. Another special feature of the Raspberry Pi is that the Windows 10 version also works on it. Since, it is a working computer that has a processor, memory, USB ports, audio output, and a graphics driver for HDMI output, and most Linux software applications can be installed on it. Such setup has many advantages, such as:

1. No need to use a separate computer as Raspberry pi is a computer itself. Also, no need to use an IO device like Arduino because Raspberry pi can handle IO directly.
2. The cost of the Raspberry is as low as USD 30 only. So, this project contains only one unit that is Raspberry Pi. So as a whole it is cheaper.
3. It can be used to see the output on the monitor by the HDMI port to plug the SBC into a TV.
4. Availability of plenty of USB ports.
5. Other peripheral devices like keyboard, mouse and printer can be added to the computer.
6. Ethernet port built onto the board helps to connect to the Internet with an Ethernet wire having ability to connect the system with current LAN or WAN.
7. Easy to change the operating system (Linux/Rasbian and Android) simply by changing the cards, owing to operating system runs from an SD card.

**Figure 3.** Raspberry Pi

3.1.3 Camera

We use a USB camera. The main reason for choosing the USB camera over the Pi camera is, first, cost effectiveness and future expansion of the proposed system. Second, the Pi camera is not preferable in our project because of its fragility. We need a long cable to move the camera to the desired location, which is verydifficult with the Pi camera with its fragile cable strip. The camera has the following features: a high-quality CMOS sensor, an image resolution of 25 MP (interpolated), an adjustable lens for focus adjustment, a frame rate of 30 fps, and an f2.0 lens. In low-light conditions, the camera has a night vision function and connects to the Raspberry Pi via the USB 2.0 port ( Fig. 2) and captures images as needed.

3.1.4 GPS/GSM module

In this era of technology, the use of GPS and GSM modules (Fig. 4) in commerce engineering, scientific use, tracking and surveillance of objects is irresistible [11]. In our project, the function of the GPS is to get

the coordinates of the automobile for tracking and GSM basically used to update the owner about the automobile location through sending and receiving SMS. The GSM-dial up, monitoring program and communication protocol are implanted together and are connected to the Raspberry pi by a serial port UART.

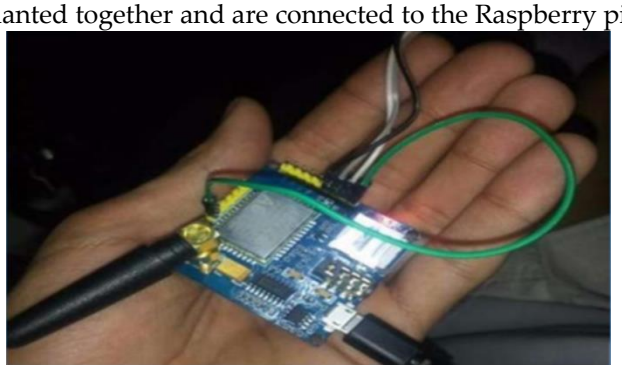


**Figure 4.** GSM/GPS module

The features of GPS/GSM module used in our project are:

1. Serial GSM/GPRS core development board based on GPRS A6 module supporting dual-band GSM/GPRS network, available for GPRS and SMS message data remote transmission.
2. Compact size and low current consumption board with power saving technique.
3. It communicates with microcontroller via UART port, supports command, including GSM 07.07, GSM 07.05 and Ai-Thinker enhanced AT Commands.

## 4. Software implementation and results

Our proposed system grant access to automobile in two ways, one is through face recognition and other through confirmation SMS. So proposed system can be categorized into two working modules that are combined together to give the expected results. The workflow is shown in Fig 5.

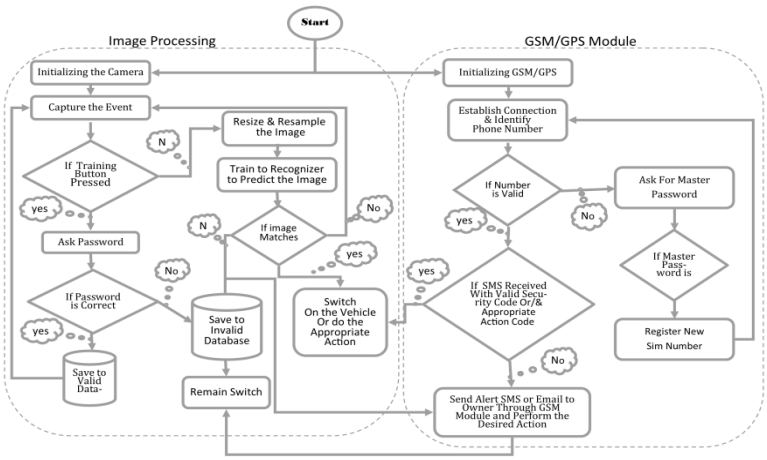



**Figure 5.** Work flow of the our proposed system model

### 4.1 Image processing

When a person gains access to the automobile, his image is essentially captured in the video stream. When the correct human face is present, the system stops recording the video streams, and the image processing modules recognize the face by comparing it to the authorized face images stored in the database. For this purpose, advanced face recognition algorithms are used for verification and validation. The Cascade Classifier algorithm defined by Paul Viola and Michael [12], which is based on hair-like features, is used for face recognition. The OpenCV library of the Python language has both a trainer and a classifier that supports the Haar cascade classifiers for face recognition. The principal component analysis (PCA) algorithm with enhanced features is used for face recognition [10].

Python's OpenCV library consists of a wide range of face recognition algorithms using the FaceRecognizer class. In the face detection phase, PCA first computes the eigenvectors and then determines the

thresholds. The Euclidean distance with respect to the thresholds of the images of unauthorized and authorized persons is compared to identify the persons. If the face is recognized (Fig. 6), i.e., if it matches the images in the database, a signal is sent to the RaspberryPi via USB and the RaspberryPi controls the lock via a relay by allowing access to the car. The issue here is whether a person is authorized to have access or is denied access if they are not. However, if the user is not authorized, but has been allowed by the owner under certain circumstances, he or she must need to train the image to be recognized by the image processing system. However, if the user is a layperson and the owner is in a remote location, adding the new person to a database can be problematic; in this situation, the second module solves the confusing situation by providing remote access.

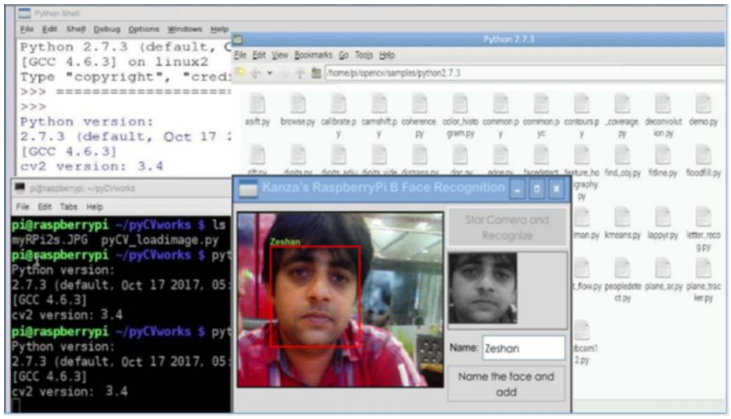


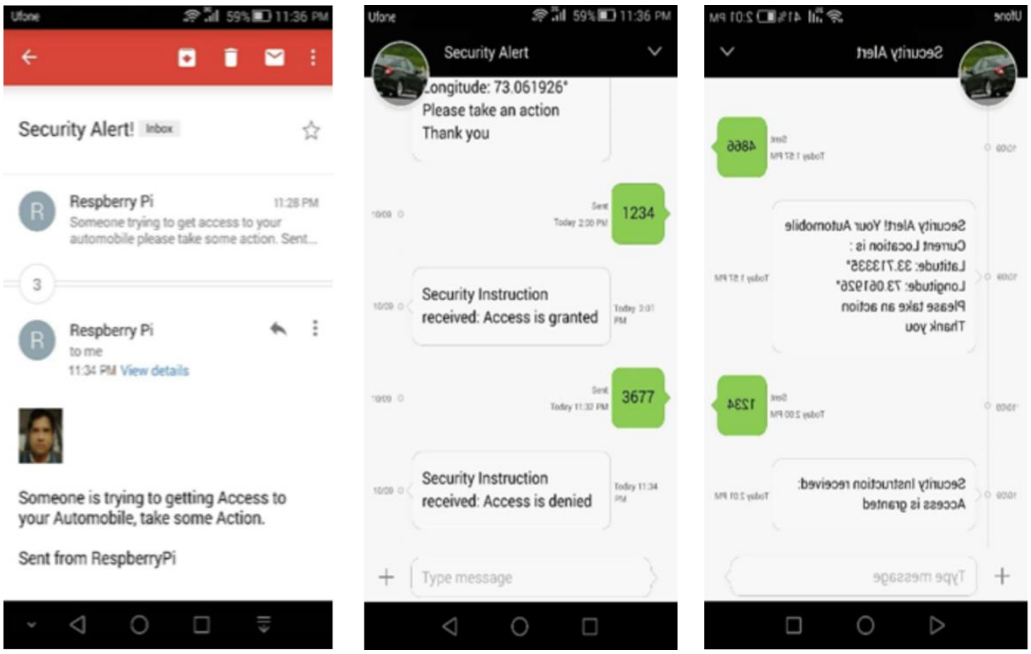

**Figure 6.** Face recognition

4.2 Remote access and monitoring

In addition to facial recognition-based authentication, we have included a GSM module to monitor remote access in the absence of the owner. If a person tries to access the vehicle, the system recognizes their face and access is denied. A warning SMS is sent to the owner's registered card number (SIM), along with the person's picture attached to the email for verification. If the owner wants to grant or deny access, he/she sends an SMS back to the system with a security code and/or the desired action code (the codes will be described later). At that moment, after cross-checking, the system performs the desired action. The system identifies the person and if it is an authorized person, access is granted.

Otherwise, the captured image is automatically transmitted via e-mail and/or a warning SMS over the GSM network to inform the vehicle owner (Fig. 7a). With the help of the GSM module, the owner can determine the location of the vehicle via GPS and perform the desired action via SMS (Fig. 7b. Via SMS, the car owner can turn the ignition of the vehicle on or off to grant or restrict access (Fig. 7c). When a location SMS is received from the owner, the tracking system sends the vehicle coordinates to the owner.

Each GPS-sensor can access GPS-satellites that are more than 24, but it should access at least 3 satellites. These satellites are one-way satellites. A GPS -receiver can receive data, but cannot send data to and from these satellites, and the data is only the exact time and approximate location of the satellites. This is because the satellites transmit at the same time. However, because of the difference in position GPS, the receiver receives the time at a slightly different interval. This difference causes the processor of a GPS receiver to calculate the distance between the satellites. Using this distance and the Pythagorean Theorem, the GPS receiver calculates longitude, latitude, altitude, time and other necessary parameters. The processor of the receiver GPS converts all calculations into a string defined as NMEA (National Marine Electronics Association) string according to the established standards. Then a serial transmitter on the receiver GPS sends this data to the serial output, in our case a UART. The algorithm written on the Raspberry Pi analyzes this string and checks if the GPS receiver can receive a sufficient number of satellites. Then our program simply analyzes the longitude and latitude. The advanced algorithm written for the proposed system works exactly according to the received instructions. The image detection, recognition and training algorithm used in [10] for image processing and GSM/GPS are presented in Algorithms 1 and 2.




(a) Email Alert (b) Remote Access (c) Location Sent

**Figure 7.** GSM module to monitor the remote access

---

Main Algorithm # 1

---

1: Initialize the camera
2: Detect if an event is captured by camera.
3: if (no image detected)
4: then (control goes to step 1)
5: end if
6: if required to train
7: then (control goes to training algorithm)
8: Compares the image captured with the images save in database to recognize the authorized person
9: if it get match
10: then (switch on the automobile)
11: Compares the image captured with the images save in database to recognize the authorized person
12: Otherwise
13: a. Remain switch off and save into invalid user database and go to step 2
14: b. Gives control to GSM module to send message to owner along with location.
15: end if
16: end if

---

The action codes followed in proposed system are given in the following.
→ 1234 to switch on the lock
→ 3677 to switch off the lock
→ 4688 to send location data to the owner
→ 4678 to send a message to police with location that car is grabbed
→ 4698 take the snap shot of the car and persons inside and send via email to owner
→ 4674 configuration like changing security code/email address/police number

**5. Discussion and Analysis**

5.1 Comparison with existing approaches in literature

After successful implementation and multiple tests, the proposed system showed encouraging results. In this section, we analyze the statistical data of the developed system in comparison with the other techniques used for motor vehicle safety reported in the literature FR. For this purpose, we analyze the performance of the system using our self-created database of 150 photos of faces. The test was repeated 80 times and the recognition accuracy is 99.2%. A slight effect of daylight is noted, but since we are concerned with FR in the car, the light available in the car is sufficient to achieve a desirable accuracy at night time. We have used PCA with advanced features that can outperform many other methods when the database is a little smaller. For the comparative analysis, we selected three OpenCV-based FR methods from the literature that are used to verify the authenticity of the user [10], [18] and [19]. The results of the analysis are shown graphically in Fig. 8. The verification rate of the system output confirms the accuracy by the ROC curve for each approach. ROC Curves are shown in Fig. 8 to confirm the performance accuracy of our proposed system.

---

Sub Algorithm #2 for GSM/GPS Module

---

1: Initialize the GSM and GPS
2: Establish connection and identify the mobile number
3: if (number is valid)
4: then see the action code and security code (go to step 5)
5: Else ask for master password
6: if (master password is correct)
7: then register the new sim number
8: if (security code received through SMS and action code is valid)
9: then (user is authorized to operate automobile) and (perform the action according to the Action received)
10: end if
11: end if
12: end if

---

5.2 Comparison with existing approaches in automotive industry

There is no affordable face recognition system for car control and security available in the market except some car companies have started installing FR and IA systems in their cars like BMW. Among other companies, Toyota has displayed a concept car with a face recognition system in a show in Paris. But there are still many lapses in adopting these systems, listed below:

a. Most of the companies are still working at the concept level. If someone wants their system to be available to the public, they have to wait for their release.
b. As we can see these systems are installed in new cars and not available in open market one must have to buy a new car with FR system.
c. Even one may have a more advanced car like having the seating of 5 persons and want to have the FR inside his/her car. But the user must also have to be limited to the luxury of the new car with FR in the same price.
d. The cars with FR system are not cheap. This price is so high that Daily Mail UK discussed the patent of FR system that Jaguar will use in land rovers. They wrote providing the technology at a low price is a challenge. In their words "It is an ongoing challenge of the automotive industry to improve vehicle functionality, design and to further enhance the sophisticated feel of vehicles, without significant additional cost".
e. Sometimes car companies also include some ongoing services like registering a person as an authentic user. In NC World article on above mentioned Jaguar patent they told. "A driver would register their biometric details when first taking ownership of the car, and these details would be referred to each time they approach the vehicle".

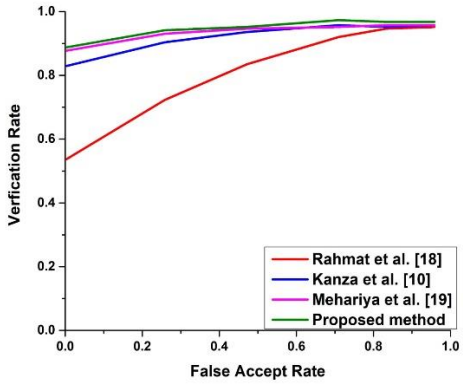



**Figure 8.** ROC curve for our proposed approach

Considering the above points, we have developed a car lock and control system that not only meets the above requirements, but also has other functions such as GSM/GPS to monitor and control the car lock remotely. Our project is not a concept, it is there, and our project is not related to a specific car. A person already having a car can just install our system and enjoy the benefits without losing the previous functions. We have developed a robust and easy to-use system that combines software with inexpensive hardware. For example, we used GSM for notification, which is a great choice because of its wide range utilities. Since SMS is a text-based protocol, we do not always need a web server for SMS or email. This may only be the case if someone wants to access their car via the Internet. In our system, the work for SMS is done in two ways (messages are sent and received) via GSM. For e-mails, we need Internet to transmit them, so they are transmitted over the network, but only in one way. However, if we want network-based two-way control and the command sender sends commands over the Internet, we need to use a web server (our command sender uses the GSM network). But for now, it lowers the cost by reducing additional components.

Also, most GSM systems are able to query the status of the vehicle and change the status according to the action code received, as well as inform the police about the location if the vehicle has been stolen. Due to the hardware and software we have chosen (OpenCV), the prices are so low that even a motorcyclist can install our security system in his vehicle. Also, the user registration is in the hands of the owner instead of having to go to the car manufacturer. The entire system is secured by a security code and authentication based on a master password. This project has great promise for the future, as users will be able to customize the system to suit their needs. The only drawback of the Raspberry Pi is that it has limited capabilities to interact with external sensors. So, a little more effort will be required in the future for a remotely controlled home security system.

## 6. Conclusion

In this paper, we have dealt with today's main problem of car theft from outside the house or a parking lot. We have developed a security system based on image processing that automatically detects the identity of the person trying to get access to the car. It prevents unauthorized entry and notifies the owner by sending a warning SMS and email with an attached photo, and allows authorized persons to enter via SMS by the owner. The developed system also provides location via GPS, to determine the current locality of the vehicle. In this way, our proposed system is the ultimate solution to all the mentioned problems. The goal of this paper is to present low-cost, customizable methods for automating security systems. In the future, we intend to use it in smart homes where the physical presence of the owner is not always secure and remote authentication and control is desired.

**Conflicts of Interest:** The authors declare no conflict of interest.

**References**


1. Mohbey, K. K. (2019). Frequent Pattern Mining Approach for a Mobile Web Service Environment Using Service Utility. Journal of theoretical and applied electronic commerce research, 14(3), 76-88.
2. Riaz, Z., Gedikli, S., Beetz, M., & Radig, B. (2009). A Unfied Features Approach to Human Face Image Analysis and Interpretation. ACII 2009 Affective Computing and Intelligent Interaction. Retrieved from https://ias.informatik. tu-muenchen.de/_media/spezial/bib/riaz09acii.pdf
3. Kenji M., & Pentland A. (1991). Recognition of Facial Expression from Optical Flow. IEICE Transactions on Information and Systems, E74-D(10), 3474–3483. Retrieved from http://search.ieice.org/bin/summary.php?id=e74-d_10_3474&category=D&year=1991&lang=&abst=
4. Spinella, E. (2003). Biometric Scanning Technologies: Finger, Facial and Retinal Scanning. San Francisco, CA, USA. Retrieved: https://www.sans.org/reading-room/whitepapers/authentication/biometric-scanning-technologies-finger-facial-retinal-scanning-1177
5. Jun, B., Choi, I., & Kim, D. (2013). Local Transform Features and Hybridization for Accurate Face and Human Detection. IEEE Transactions on Pattern Analysis and Machine Intelligence, 35(6), 1423–1436. https://doi.org/10.1109/TPAMI. 2012.219
6. Liu, S., & Silverman, M. (2001). A Practical Guide to Biometric Security technology. IT Professional, 3(1), 27–32.https://doi.org/10.1109/6294.899930
7. Kar, S., Hiremath, S., Joshi, D. G., Chadda, V. K., & Bajpai, A. (2006). A MultiAlgorithmic Face Recognition System. In 2006 International Conference on Advanced Computing and Communications (pp. 321–326). IEEE. https://doi.org/ 10.1109/ADCOM.2006.4289908
8. Padmapriya, S., & KalaJames, E. A. (2012). Real time smart car lock security system using face detection and recognition. In 2012 International Conference on Computer Communication and Informatics (pp. 1–6). IEEE. https://doi.org/10.1109/ICCCI.2012.6158802
9. Saifullah, Khawaja, A., Arsalan, H., Maryam, & Anum. (2010). Keyless car entry through face recognition using FPGA. In 2010 International Conference on Future Information Technology and Management Engineering (Vol. 1, pp. 224–227). IEEE. https://doi.org/10.1109/FITME.2010.5654862
10. Gulzar, K., Jun Sang, & Tariq, O. (2017). A cost effective method for automobile security based on detection and recognition of human face. In 2017 2nd International Conference on Image, Vision and Computing (ICIVC) (pp. 259–263). IEEE. https://doi.org/10.1109/ICIVC.2017.7984557
11. OpenCV Homepage. Available: http://opencv.willowgarage.com/wiki
12. Viola, P., & Jones, M. (2001). Rapid object detection using a boosted cascade of simple features. In Proceedings of the 2001 IEEE Computer Society Conference on Computer Vision and Pattern Recognition. CVPR 2001 (Vol. 1, pp. I-511-I–518). IEEE Comput. Soc. https://doi.org/10.1109/CVPR.2001.990517.
13. Feng, G. C., Yuen, P. C., & Dai, D. Q. (2000). Human face recognition using PCA on wavelet subband. Journal of electronic imaging, 9(2), 226-233.
14. Satonkar Suhas, S., Kurhe Ajay, B., & Prakash Khanale, B. (2012). Face recognition using principal component analysis and linear discriminant analysis on holistic approach in facial images database. Int Organ Sci Res, 2(12), 15-23.
15. Yang, B., & Chen, S. (2013). A comparative study on local binary pattern (LBP) based face recognition: LBP histogram versus LBP image. Neurocomputing, 120, 365-379.
16. Hannan, F. A., Khalid, Z., & Rafiq, A. (2018). Comparative Analysis of Face Recognition Methodologies and Techniques. NFC IEFR Journal of Engineering and Scientific Research, 4.
17. Behzad, M., Sana, A., Khan, M. A., Walayat, Z., Qasim, U., Khan, Z. A., & Javaid, N. (2014). Design and development of a low cost ubiquitous tracking system. Procedia Computer Science, 34, 220-227.
18. Rahmat, R. F., Loi, M. P., Faza, S., Arisandi, D., & Budiarto, R. (2019, June). Facial recognition for car security system using Fisherface method. In Journal of Physics: Conference Series (Vol. 1235, No. 1, p. 012119). IOP Publishing.
19. Mehariya, J., Gupta, C., Pai, N., Koul, S., & Gadakh, P. (2020, July). Counting Students using OpenCV and Integration with Firebase for Classroom Allocation. In 2020 International Conference on Electronics and Sustainable Communication Systems (ICESC) (pp. 624-629). IEEE.