Retraction

Retraction: IoT based Intelligent Car Security System using IRIS image features (*J. Phys.: Conf. Ser.* **1916** 012195)

Published 23 February 2022

This article (and all articles in the proceedings volume relating to the same conference) has been retracted by IOP Publishing following an extensive investigation in line with the COPE guidelines. This investigation has uncovered evidence of systematic manipulation of the publication process and considerable citation manipulation.

IOP Publishing respectfully requests that readers consider all work within this volume potentially unreliable, as the volume has not been through a credible peer review process.

IOP Publishing regrets that our usual quality checks did not identify these issues before publication, and have since put additional measures in place to try to prevent these issues from reoccurring. IOP Publishing wishes to credit anonymous whistleblowers and the Problematic Paper Screener [1] for bringing some of the above issues to our attention, prompting us to investigate further.

[1] Cabanac G, Labbé C and Magazinov A 2021 arXiv:2107.06751v1

Retraction published: 23 February 2022
IoT based Intelligent Car Security System using IRIS image features

G Babu¹, M Soniya²
¹ Department of Biomedical Engineering, Associate Professor, Easwari Engineering College, Chennai, Tamilnadu, India
² Technical Trainee, KPIT, Chennai, Tamilnadu, India
babutry@gmail.com

Abstract. A major crisis for car owners is that they are in persistent fear of having their vehicles stolen from parking area or outside their dwell. Connected to vehicles, cyber security takes on a much progressively imperative job such as frameworks and segments that administer security must be shielded from unsafe assaults, unapproved access and harm. Image processing based real time vehicle theft detection and prohibition system provide an optimum solution for this issue. This project provides a solution for car hacking and theft detection with the help of image processing-based application by using embedded system. All articles must contain an abstract. The IoT based iris door lock and unlock is the optimal method for the security in automative domains. From this work can understand the concepts of digital image processing and iris recognition to a greater extent.

1. Introduction
Iris recognition is the biometric identification which captures the one or more iris images of the peculiar person, this method is more reliable to identify the person more accurately as they are stable and unique. The distinctive patterns which surround the pupil of the eye can be easily identified by this technique. Security tokens, magnetic stripe cards and countersign all this information is confiding only on the data. It doesn’t provide any knowledge about the person’s peculiarity. So, the next walk is towards the biometric applications. For car security system they have implemented with face recognition techniques. In face recognition technique, if the owner is severely injured then it doesn’t detect the person. It commits mistakes when the wrinkles appear on their face. Moreover, face is same for identical twins and it is not unique. Certain complications are faced in data processing and storing. Iris provides the optimal solution for personal identification because it doesn’t require any human authority. Consequently, it is a focus point in biometric application. At the outset they started to place the camera inside the car. The motive of the person who accesses the car may not be focused only to ransack it, but also, they can do certain malfunctions such as infusing some poisonous gas into the air conditioner and break our car braking system. So the information reaches the owner only after the car is looted. In this paper, the proposed system overcome these above stated drawbacks by using image processing-based iris recognition techniques for enhancing the security. By this paper, the car owners are most benefited concerning security by eradicating these issues. [4] considered the drawbacks of using other biometric applications and provided a solution by using iris recognition.

The iris recognition is unique, reliable and more accurate to be used in mobile phones. This used techniques to detect the pupil and corneal specular reflection. For CDMA phones of ARM CPU can’t
give the valid results.[3], focused mainly on coding algorithms. By using DCT, one can freely access 2156 pictures of 308 eyes and also 2955 pictures of 150 eyes from CASIA and Bath database respectively. Through this positive false rejection rates can be obtained. [5] provided the solution for the iris recognition when the distance between the iris and the camera keeps increasing which degrades quality and resolution of the captured image. It surveyed the central dimensions of the iris picture which doesn’t change due to the external conditions. [1] contributes the problems faced in connected car. The three most important security problems in connected cars are e-mobility, car sharing and automated valet parking. This problem was overcome through ICT coverage in automotive domain. [6] proposed a vehicle can be easily accessed by the unauthorized users. In order to prevent this from the illegal person’s the features such as encryption, decryption and message authenticated were enforced by using black box, white box and grey box approaches.

2. Methodology
In order to overcome these flaws, the paper proposed a technique intelligent car security system shown in Figure 1. This technique minimizes the issues faced in car security system. It provides a solution for vehicle security issues by using iris recognition techniques in which we placed a camera outside the car. Alerting message is sent before the car is robbed. The iris images of the owner are stored in the database. If the iris image of the current user doesn’t match with existing database, then image of the person is sent to the owner via mail [2]. This is also redirected to nearby police station after confirmed by the owner. Electrical connections are deactivated immediately. If the person is the owner’s next of kin or any familiar person then the electrical connections are activated by the owner with the help of IOT. All the information is updated in the IOT. The locations of the car can be checked at any time via IOT modules. If the person access more than three times, then SMS alert is also sent to the owner [7].

3. Block diagram of the proposed method
The boundary box is used to crop the eyes of the captured image. After segmenting the eyes, it will resize the iris image according to the database. Then it will check for correlations between these two datasets. Later, it will normalize the iris image to enhance the accuracy. It will encode the local binary patterns in order to provide the security. Finally, it will check with the iris image which is stored internally. If it matches, then the car door opens and motor rotates. If the current user’s image doesn’t match with the database, then it will inspect for the attempt shown in Figure 1.

![Figure 1. Block diagram the Intelligent Car Security System](https://example.com/figure1.png)

If the attempt is less than or equal to three and if the person touches the car door again, the camera is ON. It will again start to capture the user’s image. When all the three attempts result in failure, then it
will send the captured image to the authorized person and to nearby police station. Electrical connections are deactivated. Buzzer is ON and SMS alert is also sent via GSM.

4. Result
The owner of the car checks with the person’s image whether he/ she is a next of kin or familiar person. If yes, then they can activate the electrical connections using Internet of Things. All the information such as IRIS IS MATCHED, IRIS IS NOT MATCHED, AND PERMISSION GRANTED everything is updated in IOT. Consequently, this method upgrades the security level to a much greater extent. The main function of this paper is to provide the cyber security from the hijackers. The proposed technique will eradicate the issues faced for car security in our day-to-day life. The result is explained with the suitable images as shown in Figures 2 and 3.

Figure 2. Authentication. (a) Touch sensor (b) Camera ON (c) Detection of eye region (d) Focus iris (e) Recognition of iris pattern (f) comparison with database (g) Authenticated message (i) Unlocks the door.

Figure 3. Unauthorized Case and Load Control. (a) Unauthorized Iris (b) Alert message (c) Updating in IOT (d) Load control (e) Permission granted (f) permission updated.

5. Conclusion
It is evident from the paper that the security is given to a greater extent by using iris recognition. The iris based door lock and unlock is the optimal method for the security in automotive domains. From this project we can understand the concepts of digital image processing and iris recognition to a greater extent. Using this application, we have proposed a system that uses iris recognition hastily. If security parking system does not receive a reply from a particular contact author, within the time schedule given (usually 72 hours), then it is presumed that the author has found no errors in the system. The tight publication schedule of our proceedings series does not allow SPS to send reminders or search for alternative e-mail addresses on the Internet.
References

[1] Alam J B, Islam M, Ahmed M and Uddin M S 2017 Smart anti-theft vehicle tracking system for Bangladesh based on Internet of Things 4th International Conference on Advances in Electrical Engineering (ICAAE) Bangladesh 624-628.

[2] Dexin Zhang, Li Ma, Tieniu Tan and Yunhong Wang 2003 Personal identification based on iris texture analysis IEEE Transactions on Pattern Analysis and Machine Intelligence 25,12.

[3] Donald M Monro, Zhang D and Rakshit S 2007 DCT-Based Iris Recognition IEEE Transactions on Pattern Analysis and Machine Intelligence 29, 4.

[4] S, D., & H, A. (2019). AODV Route Discovery and Route Maintenance in MANETs. 2019 5th International Conference on Advanced Computing & Communication Systems (ICACCS). doi:10.1109/icaccs.2019.8728456

[5] H. Anandakumar and K. Umamaheswari, An Efficient Optimized Handover in Cognitive Radio Networks using Cooperative Spectrum Sensing, Intelligent Automation & Soft Computing, pp. 1–8, Sep. 2017. doi:10.1080/10798587.2017.1364931

[6] Ronald E Haas and Dietmer P F Moller 2017 Automotive connectivity, cyber-attack scenarios and automotive cyber security IEEE International Conference on Electro Information Technology (EIT) 635-639.

[7] Sun H, Li Z, Zhang Q (2018) Deep Feature Fusion for Iris and Periocular Biometrics on Mobile Devices IEEE Transactions on Information Forensics and Security 13,11.