Grenze International Journal of Engineering and Technology, June Issue

Enhanced Automotive Security System

Mohamed Raziur Rahman M[1], Dinesh V[2] and Krishna N[3]
[1-3]Easwari Engineering College (Affiliated to Anna University, Chennai, Tamil Nadu, India), Department of Electronics and Communication Engineering, Chennai, India
Email: mohamedraziurrahman@gmail.com, dinesh.v@eec.srmrmp.edu.in , krishnanrynn2712@gmail.com

***Abstract*—Over the last few decades, individual transportation has increased remarkable rate at the worldwide. Increase in crime rate of vehicle theft is now a days, a challenging one. Wide spectrum of vehicle, mainly car is considered in this system. The purpose of this study greatly improves security measures by smoothly integrating face recognition, QR code, anti-spoofing in an *Enhanced Automotive Security System*. This system will help the individual to secure their vehicle from theft or unauthorized attempt, where the image will be captured by the external camera and it will be immediately sent to the owner of the vehicle, enabling them to take necessary action. By implementing this technique, is affordable when compared to expensive cars. Further QR code methodology is provided for guest access, and anti-spoofing technology is also added to this feature. This security system can be fixed in an affordable way by using, accessible components, such as camera, Raspberry Pi, Arduino, Python library, GSM Module, Relay Module, SD Card Module, Embedded C, YOLOv8 algorithm, QR Code and Chatbot.**

***Index Terms*— Facial Authentication Vehicle Systems, QR Code, Anti-spoofing, YOLOv8, Chatbot, Arduino.**

I. INTRODUCTION

The purpose of this study was to deploy effective and efficient technology by implementing *Enhanced Automotive Security System.* This system can be applied to any vehicle. This system developed in such a way to full fill the needs of a car enthusiast to enhance the vehicle security in a affordable cost. Most expensive vehicle manufacturing companies which they provide this facility default making it costlier to afford. Increase in crime rate of car theft which alarms knowledge towards this system.

The previous studies regarding biometrics technology of facial recognition security applied while the engine of the vehicle is turned on. Most of the earlier studies revealed that this technology is applied only in cars.

The extension of this system, which enhances keyless entry of the vehicle to the guest access authorization is also given by generating QR code that can be sent to the guest by the owner or authorized person to use the owner's vehicle without key. This system of vehicle security can be implemented on both two wheelers 'and four-wheeler or any other vehicles. wide spectrum of vehicle here mainly car has been taken because of more people are car enthusiasts. Face recognition sparkle a lot of attention employed in computer vision system for autonomous control and wireless communication.

Numerous vehicle security systems have been constantly improved with advancement using various embedded technologies. Main goal of this system is to provide advanced and enhanced vehicle security system using face recognition and QR code. This security system can be applied almost in all the vehicles either commercial or domestic purpose. One can extend utility of these security systems wherever needed. Car automation and

Grenze ID: 01.GIJET.10.2.507_1

surveillance is an escalating trend in this decade. Smart enhanced vehicle security is becoming indispensable need as it makes it easier for the owner to ensure the automobile safety.

A. S. Jacob et al., used the component mini–CPU Raspberry Pi which interfaces with embedded peripherals simultaneously, the vehicles can be managed through mobile phones with minimal cost. Numerous vehicle security systems have been constantly improved with advancement using various embedded technologies [1]. This security system applicable in older cars having remote keys. If an individual would like to go for further more enhanced security level, cost may increase in an affordable way when compared to in-built security system provided by the car manufacturers.

A camera sensor is mounted within the car steering column and the driver needs to confirm identity and before being able to use the key to unlock the vehicle or start the ignition [2]. The infrared sensor attached to the driver seat of the vehicle activates the hidden camera fixed in appropriate position, as soon as face of the person is detected, if the person is not authenticated, the face of the person which is classified as unknown is sent to the email of the owner as an MMS through the software [3].

The previous studies regarding biometrics technology of facial recognition security applied while the engine of the vehicle is turned on. But this study further enhances the other features and integration of cutting-edge technologies to fortify vehicle security and reshape the paradigm of modern-day.

In this system, camera is fitted outside and capture the person's image, before a driver entering inside the vehicle. It makes further advancement and easy way to secure the vehicle. Moreover, this security system on the other hand is a mode of keyless entry. According to the utility we can add more than two owners to the database, for the access of the vehicle. The QR code authorization is also given by generating QR code, can be shared to the guest by the owner or authorized person to use the owner vehicle without key. Further this study provided with anti-spoofing technology[4][5].

Santhiya. S et al., presented an advanced vehicle security system made up of face recognition using IOT platform and Python frame work. In their work where Face recognition was done while the person is seated inside the vehicle, have programmed accordingly [6].

A. Kumari Sirivarshitha et al., their study converts the mathematical aspects of a person's face into face print, to verify an individual's identification. A deep learning system, compares a digital image or an image taken quickly to a previously stored image in the data base. In this, they used designed algorithm using libraries in python [7].It is to provide system of vehicle security, real-time processing of huge amounts of data on face recognition is satisfied using CUDA (*Compute Unified Device Architecture*) [8].

Y. Cho, J. Kim, and D. Yu, they contribute to providing gold standards for the CUDA GPU parallel computation considering both computational efficiency and ease of implementation where they recommend implementing CUDA GPU parallel computation using python with either a dynamic-link library or PyTorch for the iterative algorithm [9].

H. Lou et al., proposed the better recognition precision and stability was obtained by using YOLOv8. Not only for higher precession for small size object detection but also can ensure the detection accuracy. And comparing With YOLOv5s, YOLOv8s which gives more accuracy [10]. And by another research YOLOv8 based Far Distance Face-Recognition by where they stated that far distance face can be detected quickly and more accurately. Hence declare that YOLOV8 is desirable to use in the study of face recognition [11].

II. Proposed Mechanism

In the past few years, Deep Learning computing has been derived the gold standard in the field of Machine Learning and convolutional community. Neural network plays an important role in the face recognition and other enhanced security system.

Research papers by *Laith Alzubaidi et al.,* stated that the main advantage of CNN (Convolutional Neural Network) compared to its predecessors. Which automatically detects the significant features without any human supervision. Further analyses various research papers published by different reputed publishers from the years 2019-2021 mainly focused on various deep learning platforms [12].

Faces need a lot of mathematical calculations because they are multidimensional. Therefore, creating face recognition with better accuracy and faster recognition times is one of the main criteria of this system. Each node determines whether there are faces in the image according to the data in classifiers data file which is the outcome in training procedure. This procedure takes few seconds to make the judgement of the face, is detected and the period of time is enough long for the security system to accomplish the face detection process.

It serves as an individual identity of everyone and therefore face recognition helps in authenticating any person's identity using his personal characteristics. The whole procedure for authenticating any face data is sub-divided

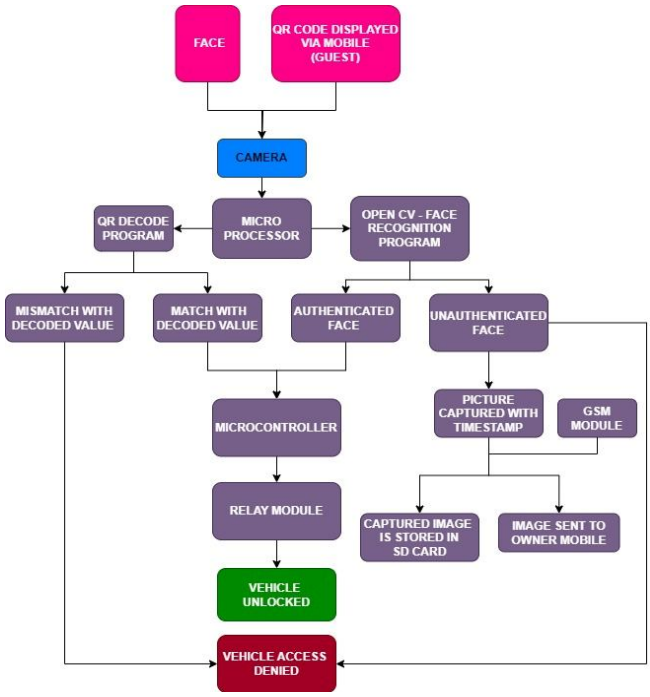

Figure 1. Block diagram of security system

into two phases, in the first phase, the face detection is done, the second phase is initiated in which the face is recognized as an individual. Then the whole process is repeated thereby helping in developing a face recognition model which is considered to be one of the most extremely deliberated biometric technology. After the face is detected the main task of face recognition system starts as to identify the known or unknown face and act accordingly. Basically, there are two type of techniques that are currently being followed in face recognition pattern that is, the *Eigenface* method and the *Fisherface method* [13].

III. Functioning of Security System

A. Face Recognition

For this biometric system, by developing programming on OpenCV/HAAR Cascade, Eigenface, Fisher Face, and python. Python coding is now a days used widely used because it is a high-level general-purpose programming. Python consistently ranks one of the most popular programming languages [14].

OpenCV library has many built-in packages which provide assistance in the facial recognition and taking up less processing time and providing increased efficiency. When OpenCV file incorporated with Raspberry Pi requires small amount of speed, fulfils the need for a cost-effective system and gives accurate result and also provide fast response to prevent any security laps [15].

Comparing the face image input with those saved in the database, if the similarity value *passes the threshold value* of true. The programme will show the face image identification and authentication [16]. For popular deep learning like PyTorch utilize GPUs heavily for training, and suffer from out of memory (OOM) problems if memory is not managed properly [17]. In this system for training data sets were performed by using CUDA 11.8 version, used RTX 3070ti GPU.

B. Authentication of the owner

Face recognition system first requires a set of database images. The first task is to create dataset of images on which the algorithm can be tested. These dataset images will be used to test the proposed algorithm which consists of 350 images. Face recognition system should have high recognition rate and high recognition speed. The aim is to select recognition algorithm that will increase the accuracy and speed up the face recognition process [18].

A real-time image acquisition by the camera mounted on the driver's door, real-time face was detected and recognized by python program. Which receives the image and analyse it with that of the trained models in the

database [19]. Once the trained database confidence value is higher than that of already trained value in the database, it will consider the face as authorised or in other words accept as an owner. (Fig 2 and Fig 3) Now the face detection and recognition program are completed.
Once the real time face is recognised by the microprocessor which will send the signal to the Arduino. When a signal is sent form the controller to the relay, the relay is switched[20]. The Arduino triggers the relay to unlock the car (green LED) and then after 20 seconds locks the vehicle again (Fig 4). This system of security can be implemented in any vehicle. So, this is one of the methods of keyless *unlocking* the car using face recognition technique.

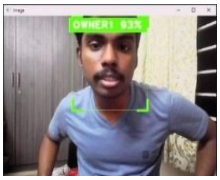

Figure 2. Identification of first owner

Figure 3. Identification of second owner

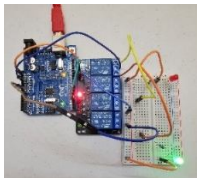

Figure 4. Arduino trigger relay to unlock for few seconds

C. Unauthorised attempt

Unauthorised person attempts to harm or try to steal the car, their image will be captured and sent to the microprocessor, for analyse with the trained models in the database. The confidence level does not match, then the microprocessor will not send the signal to the microcontroller that is Arduino. (Fig 5) The unauthenticated identification does not trigger relay to unlock the car. (Fig 6).

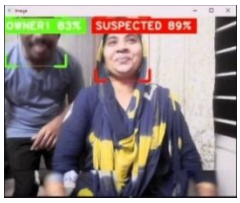

Figure 5. Identification of stranger

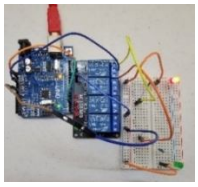

Figure 6. Arduino will not trigger the relay

Further unauthorised person's image will be sent to the car owner's mobile phone linked with the security system of the car via chat bot from the microprocessor. Then necessary steps can be taken by the car owner to protect their vehicle from theft or attempt to harm. In previous researchers and authors protect the vehicle from unauthorised attempts, either the security system will give alert as alarm, or sending email, sending MMS through software, those work have been cited. Another research paper by *Bharath Kumar et al.*, who declared in their paper about ignition on face recognition using GPS to track the location of the car, where they used Raspberry Pi and Open CV [21]

D. Anti-Spoofing

The face recognition technology is prone to failure as spoof attack and attempts are happening [22]. Recently spoofers giving more mental problems, hence to provide the protection from the spoofers', anti-spoofing technology is a must. In this study of enhanced vehicle security, anti-spoofing technology is applied.
Application such as online payment, e- commerce security, smart phone-based authentication secured access control, biometric passport and boarder checks etc., hence it is difficult to protect from such spoofing. Sometimes spoofing attacks are severe, hence researchers focused on anti-spoofing technology [23]. The spoofers cannot unlock the vehicle by showing any form of owner's virtual images in front of the camera. (Fig 7) This security feature will surely attract car enthusiasts and also other vehicle owner.
The spoofers image will be sent to the mobile phone through chat bot with timestamp on the captured image. (Fig 8) In previous researches, it is less evident that not all the details with the spoofer's image are sent to the owner of the vehicle. For this technique chat bot is interfaced with Python code using bot token.

E. QR Code

QR code (*Quick Response Code*) is a matrix of two-dimensional bar code. Denso wave incorporated by separating its QR code development division in 2001.Since then Denso Wave has been responsible for the code

Figure 7. Spoofing identified (virtual image of the owner)

Figure 8. Unauthorised attempt with timestamp

[24]. QR Code can handle up to 7,087digits. But limited work exists in the literature evaluating QR Code Scanner in the ***context of security purposes*** [25]**.** QR Code can store 7,089characters. Among 4,296 characters of alphanumeric data. 2953 bytes of binary (8bits), 1817 characters of Japanese Kanji/ Kana symbols. Which it could be scanned from any angle out of 360 degrees. This information was given by *Kammason C et al.*, 2022 in their article Dual Image QR Code [26]. QR Code generation using C library by *Phaisram Sutheebanraj and et al.*, used Drupal Module was in conjunction with the popular libqren code C library to developed user interface on the web browser and encode data in a QR Code Symbol. QR Code can be extended in the study of security system [27]. Research paper revealed that a comprehensive study of general guidelines and solutions claim to provide security and privacy characteristics and evaluate and discuss the feature of these applications [28]

F. Guest Mode Access

To authenticate guest access, owner of the vehicle will generate QR Code based on random value using chat bot from their mobile phone. Generated QR Code is then shared to the guest mobile phone. (Fig 9) The QR Code is generated by using Python environment. Guest mode feature can be achieved by sharing QR codes to the guest only by the wish of the owner. Since the QR code patent was treated as *licence -free or public domain*, it is easy to scan and apply.

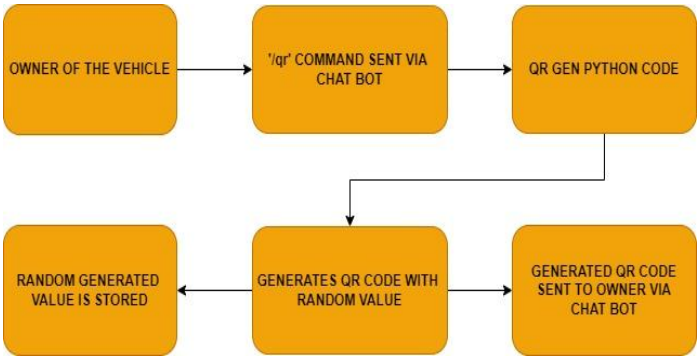

Figure 9. Block diagram for QR code Generation

G. QR Code Application

The owner of the car would like to give permission to the unauthorised guest to unlock the car for access through generating and sharing QR Code to the guest mobile phone. QR code method is used to access the car without the key or the real-time image. The QR Codes can be easily scanned by smartphone cameras. QR Code application significantly and frequently used in the digital markets [29].

The owner can make the QR code shared as invalid by generating new QR code which changes the stored generated value so that the previous QR code becomes invalid and which denies the access of the vehicle by the concerned person. Only the QR code generated is sent to the owner and the generated value will not be known even by the owner for security concerns. So always use an updated QR Code for enhanced security system of the vehicle. Here chat bot is of mediator between owner's mobile phone and microprocessor of the car's security system. The QR Code generated here is of more than four digits. (Fig 10)

QR Code received by the guest should show it in front of the camera for scanning, then it gets decoded by the QR decode python program. (Fig 11) and if the QR decoded value matches with the generated value that is

stored in the microprocessor of the security system, then the signal is sent to the microcontroller which will further trigger to unlock the central locking system.

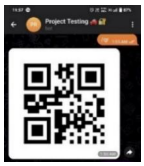

Figure 10. Authenticated QR code

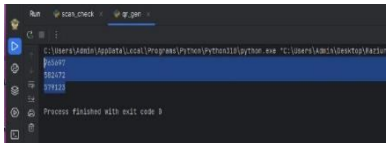

Figure 11. Verification of QR code

H. Using Invalid QR Codes

By using invalid QR Code is attempted to unlock the car, the decoded value does not match with the generated value stored in the microprocessor of the security system. Then the vehicle access will be denied. Hence this system enhanced further more security of the car to protect it from attempt to theft or harm. The print statement of invalid QR code can be seen in Figure 12.

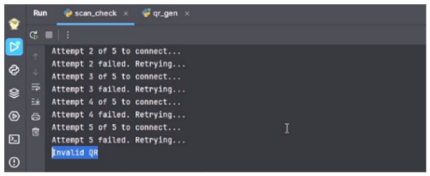

Figure 12. Invalid QR code

IV. Graphical Analysis of Training Model

Most facial expression data sets include facial and non-facial areas, and the non-facial areas probably not an essential region. Therefore, face detection is necessary to remove the nonessential areas from the input image. In this study, Retina face was employed as the face detector that demonstrates promising high-speed accuracy and high - speed performance on RGB database, including various head poses, blurs and illuminate variations. After detecting the facial area, all images were normalised to the same resolution because detected facial regions differ from person to person [30].

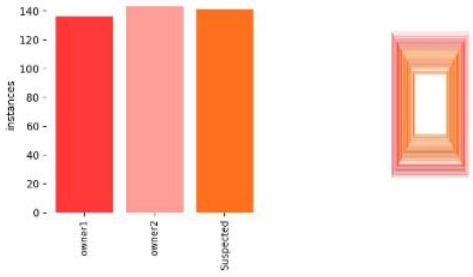

Figure 13. Label diagram of Instances of classes

In Figure 13 it is observed that, the instances of faces being detected by the model to their respective classes.
In the following Figure 14, it is observed the losses for each epoch. The losses are taken for both training and validation set. The distribution focal loss considers the problem of class imbalance while training and in Figure 15, it is observed the losses, precision, recall and mean average precision for each epoch. For Metrics/mAP50(B) the mean Average Precision at 50% Intersection over Union (IoU) for a bounding box and also it calculates average precision at a specific IoU threshold and for Metrics/mAP50-95(B), the mean Average Precision at 50% to 95%.
The Figures from 16 & 17, uses formula to get the precision, recall, the F1 with the values like True Positive (TP) – model predicted and it is correct, False positive (FP) – model predicted and it is incorrect, False Negative (FN) – model predicted and it is incorrect, True Negative (TN) – model predicted and it is correct to calculate and here x axis is taken as confidence normalized values for the Figures.

$$precision = \frac{(true\ positive)}{(true\ positive) + (false\ positive)} \quad (1)$$

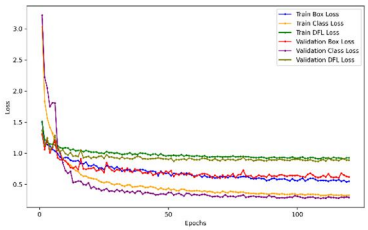

Figure 14. Training and Validation loss Over Epochs

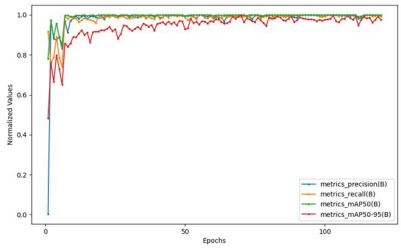

Figure 15. Metrics Graph

$$Recall \frac{(true\ positive)}{(true\ positive) + (false\ negative)} \quad (2)$$

$$F1\ score = \frac{(precision \times Recall)}{[precision + Recall]/2} \quad (3)$$

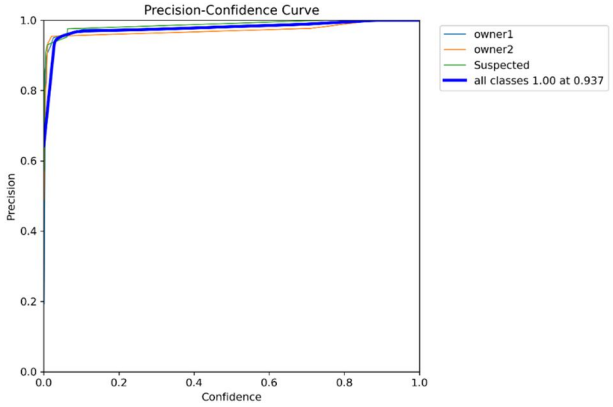

Figure 16. Precision Confidence Curve

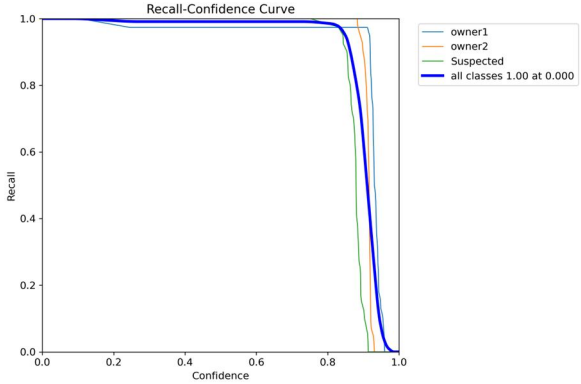

Figure 17. Recall-Confidence Curve

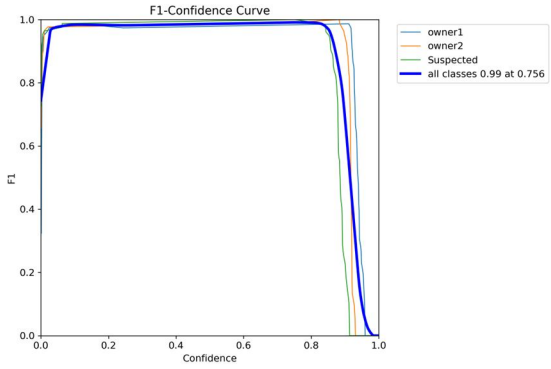

Figure 18. F1-Confidence Curve

Further, in Fig 18, observed the F1 score which gives us measure of model accuracy in statistical analysis. By using the formula (3), the F1 score is calculated with the values of precision and recall. Then the graph taken as confidence curve in x axis and F1 score in y axis to get F1-confidence curve.

V. CONCLUSION

More than 350 training datasets were considered, image captured from 3to 5 feet and achieved up to 92 percent of accuracy. This study mainly focused to secure the vehicle from outside and inside hence the camera is used outside. To overcome hacking attempts here we implemented anti-spoofing technology.

Car manufacturers are concentrating more on safety and security by providing advanced automated technologies in the competitive world of business. Anti-spoofing, QR technology is a modern and sophisticated system of higher level enhances keyless entry. This can be applied on any valuable property where safety is a threatening one.

Our proposed Enhanced Automotive Security System affordable to individual car owners to cab owners. QR code is another best feature to secure the vehicle, but limit the authorised users to ensures privacy and hassle-free lifestyle. This level of security system may one of the ways to reduce city car crime and further promotes towards evolution of smart city concept.

ACKNOWLEDGMENT

I give the Almighty my heartfelt gratitude for leading me on this path. We are especially grateful for the support of Easwari Engineering College. I really thank supervisor Dinesh V for his insightful guidance. My teammate Krishna N contributed to this work, for which I am grateful. Many thanks to friends for their support and encouragement. Finally, I want to express my sincere gratitude to my family for their constant support and belief.

REFERENCES

[1] S. Jacob, V. Chaurasiya, V. Sharda, and S. Dixit, “Car surveillance security system,” in 2017 International conference of Electronics, Communication and Aerospace Technology (ICECA), IEEE, Apr. 2017, pp. 735–739. doi: 10.1109/ICECA.2017.8203640.

[2] H. Biswas, V. Sarkar, P. Sen, and D. Sarddar, “Smart city development: Theft handling of public vehicles using image analysis and cloud network,” in Recent Trends in Computational Intelligence Enabled Research, Elsevier, 2021, pp. 155–169. doi: 10.1016/B978-0-12-822844-9.00013-X.

[3] K. K. Dube, P. S. Satalkar, D. V Warule, and S. T. Patil, “FACE RECOGNITION SYSTEM FOR UNLOCKING AUTOMOBILE USING GSM AND EMBEDDED TECHNOLOGY,” International Research Journal of Engineering and Technology, 2019, [Online]. Available: www.irjet.net

[4] S. P. P. K. R. V Dinesh, “SPK- A Traffic Violation Detection System,” International Conference on Human Machine Interaction in the digital era (ICHMIDE 2023), 2023.

[5] G. M. V Dinesh, “Detection of People or Animals Using Deep-learning in Railway Tracks,” International Conference on Human Machine Interaction in the digital era (ICHMIDE 2023), 2023.

[6] S. S, D. T, J. J, and K. D, “Improved Authentication and Drowsiness Detection from Facial Features using Deep Learning Framework in Real Time Environments,” in 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, Mar. 2023, pp. 1638–1642. doi: 10.1109/ICACCS57279.2023.10112846.

[7] A. Kumari Sirivarshitha, K. Sravani, K. S. Priya, and V. Bhavani, “An approach for Face Detection and Face Recognition using OpenCV and Face Recognition Libraries in Python,” in 2023 9th International Conference on Advanced Computing and Communication Systems (ICACCS), IEEE, Mar. 2023, pp. 1274–1278. doi: 10.1109/ICACCS57279.2023.10113066.

[8] J. Xu and S. Wu, “Parallel research of shape context face recognition algorithm based on CUDA,” in 2011 International Conference on Consumer Electronics, Communications and Networks (CECNet), IEEE, Apr. 2011, pp. 3319–3323. doi: 10.1109/CECNET.2011.5768177.

[9] Y. Cho, J. Kim, and D. Yu, “Comparative Study of CUDA GPU Implementations in Python With the Fast Iterative Shrinkage-Thresholding Algorithm for LASSO,” IEEE Access, vol. 10, pp. 53324–53343, 2022, doi: 10.1109/ACCESS.2022.3175987.

[10] H. Lou et al., “DC-YOLOv8: Small-Size Object Detection Algorithm Based on Camera Sensor,” Electronics (Basel), vol. 12, no. 10, p. 2323, May 2023, doi: 10.3390/electronics12102323.

[11] F. Gunawan, C.-L. Hwang, and Z.-E. Cheng, “ROI-YOLOv8-Based Far-Distance Face-Recognition,” in 2023 International Conference on Advanced Robotics and Intelligent Systems (ARIS), IEEE, Aug. 2023, pp. 1–6. doi: 10.1109/ARIS59192.2023.10268512.

[12] L. Alzubaidi et al., “Review of deep learning: concepts, CNN architectures, challenges, applications, future directions,” J Big Data, vol. 8, no. 1, p. 53, Mar. 2021, doi: 10.1186/s40537-021-00444-8.

[13] G. Singh and A. K. Goel, “Face Detection and Recognition System using Digital Image Processing,” in 2020 2nd International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), IEEE, Mar. 2020, pp. 348–352. doi: 10.1109/ICIMIA48430.2020.9074838.

[14] M. Khan, S. Chakraborty, R. Astya, and S. Khepra, “Face Detection and Recognition Using OpenCV,” in 2019 International Conference on Computing, Communication, and Intelligent Systems (ICCCIS), IEEE, Oct. 2019, pp. 116–119. doi: 10.1109/ICCCIS48478.2019.8974493.

[15] Umm-e-Laila, M. A. Khan, M. K. Shaikh, S. A. bin Mazhar, and K. Mehboob, “Comparative analysis for a real time face recognition system using raspberry Pi,” in 2017 IEEE 4th International Conference on Smart Instrumentation, Measurement and Application (ICSIMA), IEEE, Nov. 2017, pp. 1–4. doi: 10.1109/ICSIMA.2017.8311984.

[16] M.-J. Wu, Y.-C. Chen, Y.-S. Liao, J.-A. Chen, and H.-H. Lin, “Face-recognition System Design and Manufacture,” in 2021 IEEE/ACIS 22nd International Conference on Software Engineering, Artificial Intelligence, Networking and Parallel/Distributed Computing (SNPD), IEEE, Nov. 2021, pp. 158–161. doi: 10.1109/SNPD51163.2021.9705014.
[17] J. Choi, H. Y. Yeom, and Y. Kim, “Implementing CUDA Unified Memory in the PyTorch Framework,” in 2021 IEEE International Conference on Autonomic Computing and Self-Organizing Systems Companion (ACSOS-C), IEEE, Sep. 2021, pp. 20–25. doi: 10.1109/ACSOS-C52956.2021.00029.
[18] N. R. Borkar and S. Kuwelkar, “Real-time implementation of face recognition system,” in 2017 International Conference on Computing Methodologies and Communication (ICCMC), IEEE, Jul. 2017, pp. 249–255. doi: 10.1109/ICCMC.2017.8282685.
[19] R. K. S. K. S. V Dinesh, “Detection and Notification system in Emergency Vehicles for unidentified accident victims,” International Conference on Human Machine Interaction in the digital era (ICHMIDE 2023), 2023.
[20] A. Khan, A. Al-Zahrani, S. Al-Harbi, S. Al-Nashri, and I. A. Khan, “Design of an IoT smart home system,” in 2018 15th Learning and Technology Conference (L&T), IEEE, Feb. 2018, pp. 1–5. doi: 10.1109/LT.2018.8368484.
[21] Bharath Kumar M, Vamshi Krishna S, V S Sai Aravind T, Pavan Kumar P, and Naresh Babu V, “Machine Learning Trained Face Recognition based Automotive Ignition System,” International Journal of Engineering Research and Technology, vol. V9, no. 04, Apr. 2020, doi: 10.17577/IJERTV9IS040488.
[22] P. Anthony, B. Ay, and G. Aydin, “A Review of Face Anti-spoofing Methods for Face Recognition Systems,” in 2021 International Conference on INnovations in Intelligent SysTems and Applications (INISTA), IEEE, Aug. 2021, pp. 1–9. doi: 10.1109/INISTA52262.2021.9548404.
[23] Z. Ming, M. Visani, M. M. Luqman, and J.-C. Burie, “A Survey on Anti-Spoofing Methods for Facial Recognition with RGB Cameras of Generic Consumer Devices,” J Imaging, vol. 6, no. 12, p. 139, Dec. 2020, doi: 10.3390/jimaging6120139.
[24] K. Katsura, “QR codes as teaching tools,” in M-Libraries 4, Facet, 2014, pp. 101–112. doi: 10.29085/9781783300037.014.
[25] R. Dudheria, “Evaluating Features and Effectiveness of Secure QR Code Scanners,” in 2017 International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC), IEEE, Oct. 2017, pp. 40–49. doi: 10.1109/CyberC.2017.23.
[26] Kammason, Y. Wanna, K. Wiratchawa, and T. Intharah, “Dual Image QR Codes: The Best of Both Worlds,” in 2022 International Conference on Digital Image Computing: Techniques and Applications (DICTA), IEEE, Nov. 2022, pp. 1–8. doi: 10.1109/DICTA56598.2022.10034633.
[27] P. Sutheebanjard and W. Premchaiswadi, “QR-code generator,” in 2010 Eighth International Conference on ICT and Knowledge Engineering, IEEE, Nov. 2010, pp. 89–92. doi: 10.1109/ICTKE.2010.5692920.
[28] H. A. M. Wahsheh and F. L. Luccio, “Security and Privacy of QR Code Applications: A Comprehensive Study, General Guidelines and Solutions,” Information, vol. 11, no. 4, p. 217, Apr. 2020, doi: 10.3390/info11040217.
[29] S. Jain, S. Chand, S. K. Sharma, and R. Jindal, “Styled-QReal: A real-time technique for QR code stylisation,” in 2023 International Conference on Computer, Electronics & Electrical Engineering & their Applications (IC2E3), IEEE, Jun. 2023, pp. 1–6. doi: 10.1109/IC2E357697.2023.10262640.
[30] D.-H. Lee and J.-H. Yoo, “CNN Learning Strategy for Recognizing Facial Expressions,” IEEE Access, vol. 11, pp. 70865–70872, 2023, doi: 10.1109/ACCESS.2023.3294099.