ISSN: 2249-7196
IJMRR/ july 2023/ Volume 13/Issue 3/Article No-1/01-10
Dr.S. Jagadeesh/ International Journal of Management Research & Review

A System for Authenticating Student ID Card (SASIC) Using Deep Learning Techniques

Dr.S. Jagadeesh[1]
Keerthika Peravali[2], Srinitha Akula[3], Divya Arrolla[4]
[1]*Professor, Department of Electronics and Communication Engineering*
[2,3,4]*B. Tech Student, Department of Electronics and Communication Engineering*
[1]jaga.ssjec@gmailcom
[2]Keerthika1926@gmail.com
[3]akula.srinitha01@gmail.com
[4]arrolladivya2001@gmail.com

***Abstract*— In educational institutions, using student identification cards for a variety of functions, including identity verification and access control to campus resources and attendance monitoring, is a standard practice. Enhancing the security and precision of student identification systems has become more and more important in recent years. As a result, sophisticated technologies like face recognition and QR code mapping have been incorporated into authentication techniques. The technology consists of two parts: the first part maps the QR code on the student ID card to a special identification number for the individual student. To confirm the identification of the student presenting the ID card, the second component uses facial recognition technology. The system's goal is to reduce the incidence of identity fraud and increase the reliability of student identification verification. To map the QR code on the student ID card to the appropriate student identity, the suggested method makes use of deep learning techniques. To determine if a student is wearing an ID card or not, the system also employs a method known as YOLOV5. Since the system can instantaneously access the student's information by scanning the QR code, it enables quick and precise identification of pupils. The suggested system includes increased precision in confirming identities of pupils, a decrease in fraud-related cases, and increased effectiveness in recording attendance and access control. If he or she enters the educational institution using their separate unique ID card, attendance is tracked on an Excel page and a welcoming chime is sounded. The technology sounds an alert and delivers an e-mail to the campus administrator with the person's photograph if an unauthorized person or pupil without an ID tries to get into the institution.**

Keywords— Student ID card Authentication, Face Recognition, QR Code, YOLOV5, Deep Learning Technique, Attendance.

I. INTRODUCTION

For the safety, security, and effective administration of campus resources in educational institutions, precise identification and authentication of students are essential. Paper-based ID cards and other outmoded traditional forms of identification are more vulnerable to abuse and fraud. Educational institutions are increasingly implementing student ID card authentication systems to help them overcome these obstacles. These systems make use of cutting-edge technology to improve campus security and streamline different administrative procedures.

In order to confirm students' identities, a student ID card authentication system is a complete solution that integrates actual ID cards with electronic authentication techniques. For student verification, institutions typically use a variety of tools, including security cameras [1], lock systems [1], RFIDs [2], [3], iris recognition systems [3], [4], and fingerprint recognition systems [5]. Educational institutions can track attendance and offer access control to limited areas by integrating these technologies. They can also verify the identity of students.

Utilizing various biometric tools, such as iris and facial recognition, thumb print identification, and other tools, is a frequent approach [8] – [12] for the verification of students. Institutions can authenticate the identification of their pupils with these solutions in a successful manner. Due to variations in human position [6], expressions of the face [7], haircuts [8,] ambient lighting [9], person proximity to the camera's lens [10], and other factors, it can be difficult to identify users in real-time utilizing these biometric methods. Due to these circumstances, erroneous alerts are generated throughout the authentication procedure.

To cut costs associated with user identification, many educational institutions choose the use of straightforward identification cards that staff members and students are required to wear as part of their attire. Due to the emphasis on monitors for hand verification, where photographic manipulation can be utilized to produce fraudulent cards that are difficult to distinguish with human perception, this tedious verification procedure is ineffective and creates security flaws.

Verifying a person's identity via a student card is a widespread practice. The visual characteristics of student ID cards can be analyzed using deep learning models, such as convolutional neural networks (CNNs) and YOLOV5. Due to their capacity to handle complicated patterns and variances in data, deep learning algorithms are increasingly being employed to authenticate student ID cards. A camera records a student's face when they give their ID card, and technologies like deep neural networks are used to extract facial information.

Making ensuring that only persons with permission can access campus facilities and services is the main objective of a student identification badge validation system. The possibility of unauthorized access or impersonation can be considerably decreased by asking students to show their ID cards and identify themselves through a safe and automated mechanism. Additionally, by doing away with manual procedures and cutting down on delays, these technologies offer students an effortless experience, thus increasing production and efficiency.

We provide an automated, inexpensive method to verify the identity of the students in order to overcome these issues. The system can use a webcam to recognize ID cards and figure out whether someone is wearing one as required by the attire rule. It can also scan the QR code on an ID card to see if the student's information is stored in the college database using deep learning techniques. The pupil's attendance is noted on the spreadsheet page if the student's profile coincides with that in the college's database. The technology will automatically send an email with a photograph of the student or unauthorized person as person without ID card found to the college administrator and play an alert sound if it detects either of these situations.

II. LITERATURE SURVEY

The mechanisms for student authentication and attendance tracking that are now in place are reviewed in this section. For student verification, existing methodologies have suggested biometric equipment [14]-[20] or RFID-based technologies [22] - [25]. An RC522 card scanner and a tag equipped with RFID are both employed in the Rf-based system for attendance. The number of attendees for the specific day is recorded when students or staff members hold their RFID card or tag above the reader. [26][27]

Yazid and his team's next system included a facial recognition system, a GPS system, and a QR code system for authentication. This system was designed to track user attendance. In order to make the entire process safer and more effective, the suggestion was primarily intended to prevent attendance via proxy. [28] By combining a fingerprint reader with GPS, which sent the user's location to their smartphone, Lia Kamelia and team created a system that was comparable to this one [29][30].

Next, Vasutan Tunbunheng from PIM in Thailand proposed using forms from Google Sheets with speech analysis. By speaking out each student's student code and using program that recognizes speech to determine whether it was present in the Google Sheet, the system was put into place to track tardy pupils [31]. The use of smartphones for employment identification is suggested by a few methods [32] [33], which also include vocal and recognition of fingertips. According to this study, 95% of the time, speech recognition results in a mistaken positive, while only 5.88% of the time, verifying fingerprints results in a false negative. A computer-based attendance control module and an interactive fingerprint capture component are included in the cordless fingerprint absenteeism system [34] built around ZigBee architecture.

A face detection technique is then applied to the frames or images created from footage tapes of the classroom, according to an approach described in a different study [35]. Recognition of facial features is used in a web-based program for a system to track attendance [36]. K-NN and deep metric learning are used to identify student encounters, while Convolutional Neural Network (CNN) is utilized to recognize faces in images that have been taken. The suggested solution in [37] attempts to collect attendance when the student reads the designated QR code using any QR scanner program, giving rapid access to the form on Google with the information needed to take attendance.

For user recognition and categorization, current technologies have made use of a combination of deep learning and traditional machine learning methods [38] - [41]. As a result of the possible advantages of improving reliability, deep learning techniques are used [42], [43].

Our proposed system is implemented using OpenCV framework, QR code mapping, deep learning algorithms like CNN and YOLOV5. To guarantee precise recognition and validation of student ID cards, this entire solution combines the capabilities of image processing, machine vision, and deep learning algorithms. To improve the quality of ID card photos, reduce noise, and get them ready for the next steps in the authentication process, image preparation techniques can be used with OpenCV. To isolate the ID card region for additional processing, the system uses OpenCV's object detection capabilities to locate and recognize student ID cards inside an image. To identify and decode QR codes from student ID cards for QR code mapping, OpenCV's QR code module is used. With the aid of this module, the system can identify QR codes in pictures or video frames and retrieve the data they contain. To improve the system's capabilities for

authentication and mapping, deep learning techniques like
CNN and YOLOv5 have been included. Using CNN models, distinguishing patterns, logos, and security characteristics particular to each ID card design are extracted from the student ID cards. The legitimacy of the ID card is subsequently confirmed by comparing these attributes to previously recorded or stored features in the system's database. In order to find and localize student ID cards and QR codes in the photos, YOLOv5, a cutting-edge object identification model, is utilized. The model can recognize and locate these things in real-time or very close to real-time because it was trained on annotated datasets containing photos of ID cards and QR codes.

Finally, our proposed system can give better security to the educational institutions in the process of student authentication. Our system ensures that one should wear his/her own ID card and it won't allow any fraudulent activities as it can detect automatically if such things happen.

III. A SYSTEM FOR AUTHENTICATING STUDENT ID CARD (SASIC) USING DEEP LEARNING TECHNIQUES

A thorough explanation of the suggested methodology is provided in the following paragraphs. Fig.1 shows the flow of our

implemented method.

A. Dataset Preparation

We gathered a sizable collection of student ID card photos, which we then bounding box annotated with respect to the classes they corresponded with. To provide reliable training, the dataset contains a variety of ID card layouts, angles, and lighting situations.

B. Pre-processing

To record input, we made use of a laptop equipped with a front-facing camera with a 1280x720 image quality. An optimized and standardized process is used to prepare the ID card image and related data. As a result, the student ID card authentication procedure is more reliable overall, feature extraction is more accurate, noise or variation-related mistakes are reduced, and feature extraction faults themselves are minimized.

C. CNN

The extraction of significant features from ID card photos and the facilitation of the verification process are made possible by CNN (Convolutional Neural Network), which is essential for student ID card authentication.

1. Feature Extraction:

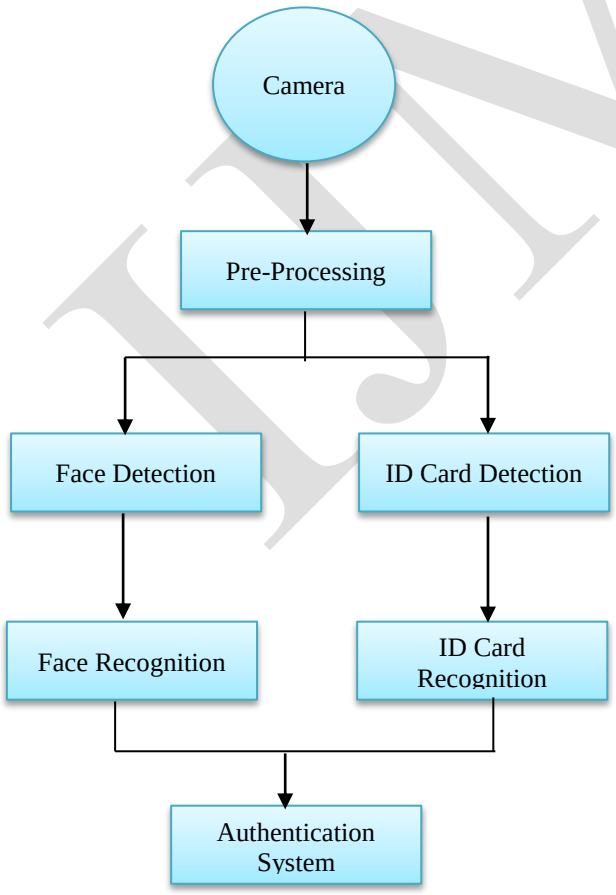
CNNs can be taught to recognize pertinent visual patterns, such as logos, text, images, or security features, that are exclusive to each ID card design. CNN can distinguish between legitimate and fake ID cards with accuracy by becoming familiar with these distinguishing characteristics.

2. Pattern Recognition:

CNNs are excellent at picking up on subtle differences and complicated patterns in photos. It will recognize graphic elements, including the college's seal, the student's picture, or protection structures, on student ID cards. By identifying these patterns and cntrasting the retrieved properties with those kept in the database, CNN can assist in confirming the legitimacy of an ID cards.

3. Generalization:

Our findings CNN can generalize their understanding and precisely extract features from brand-new, unseen ID cards after being trained on a representative collection of ID card images. Without the need for explicit programming for each unique design or variation, the system can efficiently authenticate ID cards due to its generalization feature.



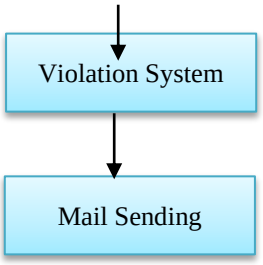


Fig. 1 Proposed System Block Diagram

D. YOLOV5

To find and locate student ID cards within an image, the YOLOv5 model is trained using the annotated dataset. The model recognizes the distinctive visual characteristics of ID cards as we train it, and it produces bounding box coordinates and class probabilities.

1. ROI Extraction:

The region of interest (ROI) containing the ID card is extracted from the image using the bounding box coordinates once the ID card has been identified using YOLOv5. In order to minimize computational overhead, the ROI extraction makes sure that only the pertinent area of the image is processed further

2. Comparing and confirming feature sets:

The pre-registered or stored features of the real student ID cards in the system's database are contrasted with the features retrieved from the CNN model. In order to gauge how closely the extracted features and the stored features resemble one another, similarity measures are computed in this step.

3. Authentication Decision:

The system determines whether to authenticate a user based on the similarity measure it acquired in the preceding phase. The student ID card is regarded as genuine, and the authentication is successful if the similarity surpasses the threshold. Otherwise, the card can be marked as dubious, necessitating further verification procedures or user intervention.

Finally, we observed that, by combining YOLOV5 for object detection and CNN model for feature extraction, the authentication system can leverage the strengths of both approaches to achieve robust and efficient identification and verification processes.

E. QR Code Mapping:

By providing precise and effective decoding and verification procedures, deep learning can significantly contribute to QR code mapping during student ID card validation.

1. QR Code Detection:

In this method, YOLO algorithm especially used to train and locate the QR code within an image. With the help of this model, which recognizes the distinctive patterns and characteristics of QR codes, it is possible to precisely pinpoint the location of the code within an ID card image. This step is very crucial in our proposed model as it is further used for decoding and verifying.

2. QR Code Decoding:

Once the QR code is detected, to analyze the QR code image and retrieve the encoded data, we used a CNN model. To ensure successful decoding, this model aids in understanding the intricate structures and patterns seen in QR codes. It also includes mistake correction capabilities.

3. Verification and Authentication:

Algorithms based on deep learning will compare the information that has been extracted with the system's stored data after the QR code has been decoded. In this phase, the decoded information—like student ID numbers or encrypted authentication tokens—is compared to the relevant database records. To ensure that the supplied QR code is connected to the appropriate student ID and confirm the legitimacy of the ID card, we trained the models to carry out these comparisons quickly

and accurately.

4. Error Correction:

Due to printing imperfections, environmental conditions or scanning issues QR code may suffer from errors. So, we trained the model to handle error correction within the QR code image using neural network-based model called autoencoder as shown in Fig.2.

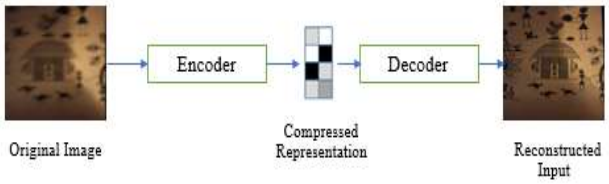


Fig.2 Autoencoder

F. OpenCV:

OpenCV offers various functions for image preprocessing like resizing, cropping and color manipulation. These techniques are applied to student ID card images to enhance their quality. It also provides functions for object detection and localization as it isolates the ID card region. OpenCV detects and decodes the QR codes from the input image and extracts the encoded information.

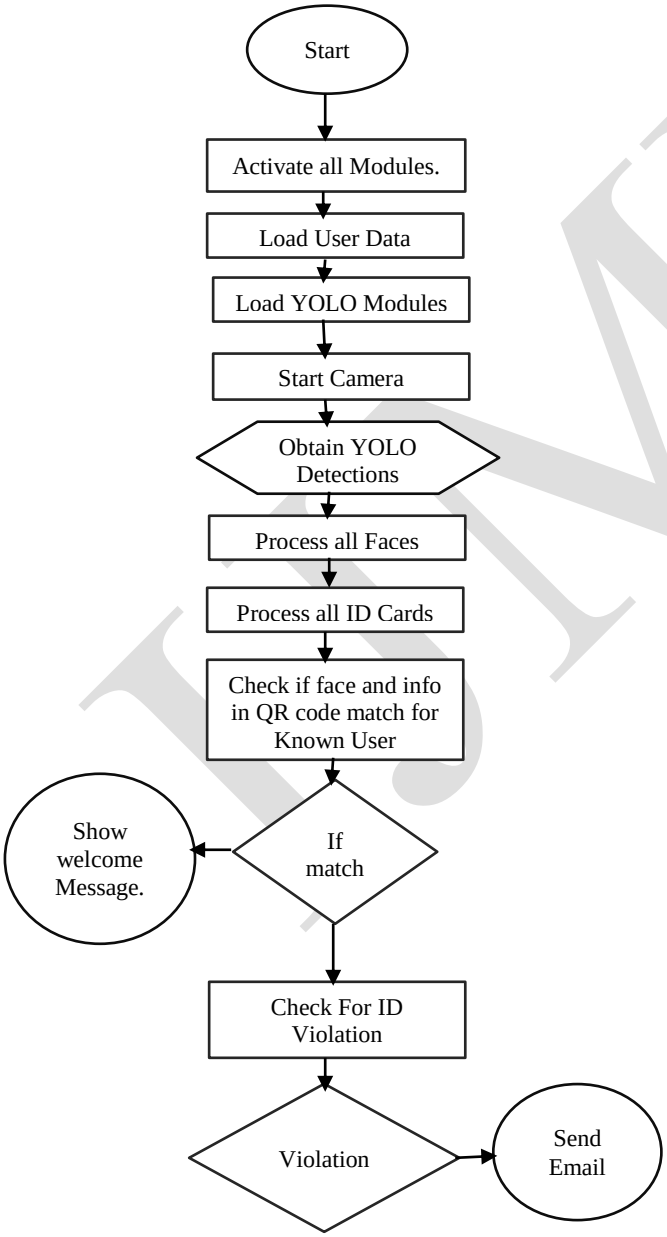


Fig.3 Activity Diagram

G. LBPH Algorithm:

We used the LBPH algorithm as it helps in giving accurate results while recognizing the face. Sparse Coding (SC), Local Binary Pattern (LBP), Histograms of Oriented Gradients (HOG), Linear Discriminant Analysis (LDA), and Gabor feature algorithms are just a few of the many face recognition methods that have been created over the years by numerous academics. A 50% to 76% accuracy percentage is offered by each of these algorithms. The LBPH algorithm, in contrast to the techniques mentioned above, has a 90% accuracy rate for both front and side face recognition.

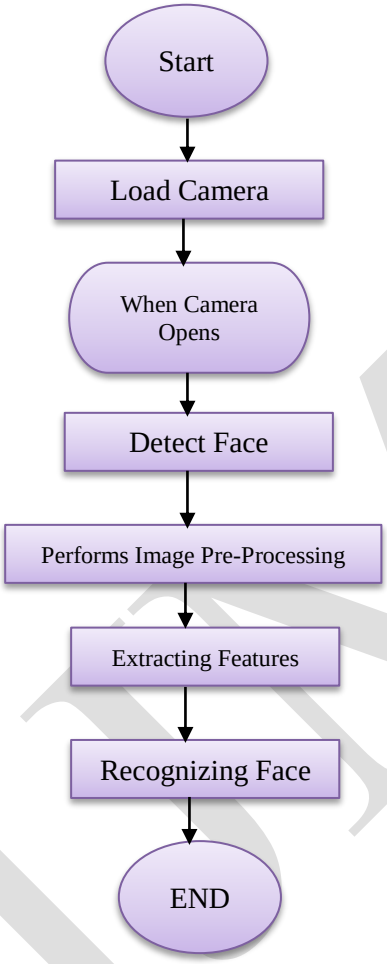


Fig.4 System Flow Diagram

For detecting faces, we have used OpenCV, which offers a Haar cascade classifier. Multiple facial traits are detected by the Haar cascade classifier using the AdaBoost algorithm.

G. Mail Sending:

We imported smtplib and given sender email and receiver email. So, when the student without ID card is detected then automatically it sends the email to the receiver. Finally, the system records the details of that student in an excel sheet. Fig.5 shows the Mail processing model.

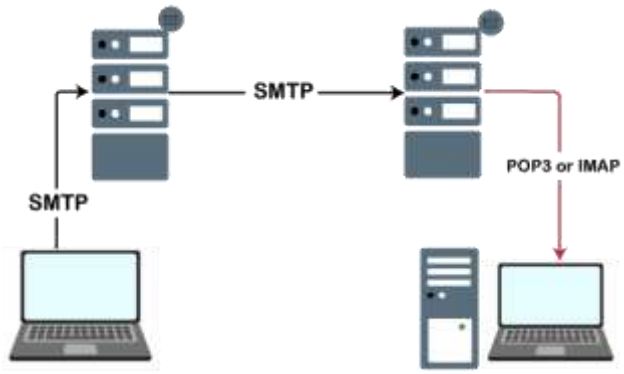


Fig.5 Mail Processing Model

H. Attendance Recording:

Our system automatically records the attendance if a student got detected with his/her own ID card. The system checks whether the student wearing his/her own ID card or not and retrieves the information from the QR code, which is in the ID card, if the student data matches with the database, then the attendance is recorded directly in excel sheet.

I. Training Mechanism:

In the first step, we collected a diverse and representative set of students with ID card images from our educational institute. We made data annotations manually. Before training we preprocessed those all images to ensure that images are in a suitable format for training. We applied deep learning models like YOLOV5 and CNN for object detection and for extracting the features from the QR code and input image. So, that system can detect automatically.

Fig.6 Trained Dataset

Fig.7 Student ID card with the QR code

IV. RESULTS

The effectiveness of the planned work is evaluated by the detection of correct credentials of the student. All educational institutions always look for providing a safe, secure, and quality education to all learning students. So, our proposed implementation can give an assurance to all the educational institutes that there is no requirement of traditional verification of a person. Our work can automatically verify whether the student belongs to their respective educational institute or not. Implementation of new work not only depends on advancement and latest technologies that is used for effective verification, but it also needs to check whether they are following rules and regulations during the process of verification. So, our method also sees whether the student is wearing his or her own ID card to avoid fraudulent activities to make the institute more secure. In our experiment, we also provided respective QR codes to the students in their ID cards. So, it will provide more security and won't allow any fraudulent activities.

The system saves the face image of the student along with his/her own ID card during the enrollment process in the database. So, during the verification process the system automatically verifies the person along with the ID card so that it detects the QR Code and check for the details whether it is matching the database and shows the welcome message, also records the attendance of that person. If student doesn't wear Id card or unauthorized person tries to enter then it plays a violation sound and sends the email to the college admin.

Now let's see the step-by-step process of the work which we implemented.

Step-1: First the student should enroll with name and ID number. So that the data is stored in the database.

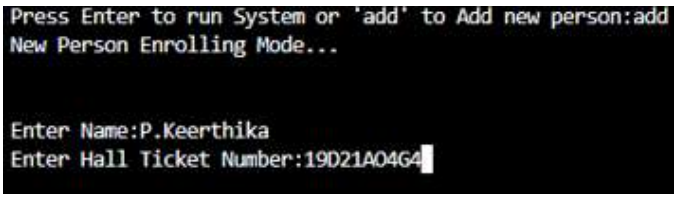


Fig.7 Enrolling Mode

Step-2: Once giving the details if we press enter then automatically webcam opens to detect face and for saving the face.

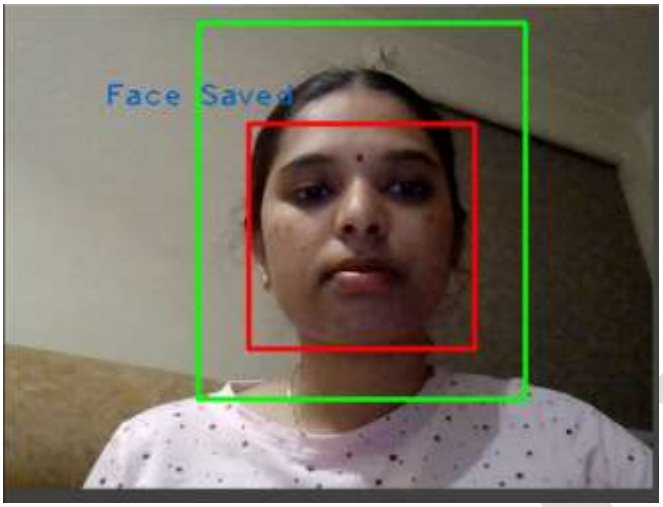


Fig.8 Saving Face

Step-3: Next also wear the ID card then webcam detects the ID and saves the ID card too.

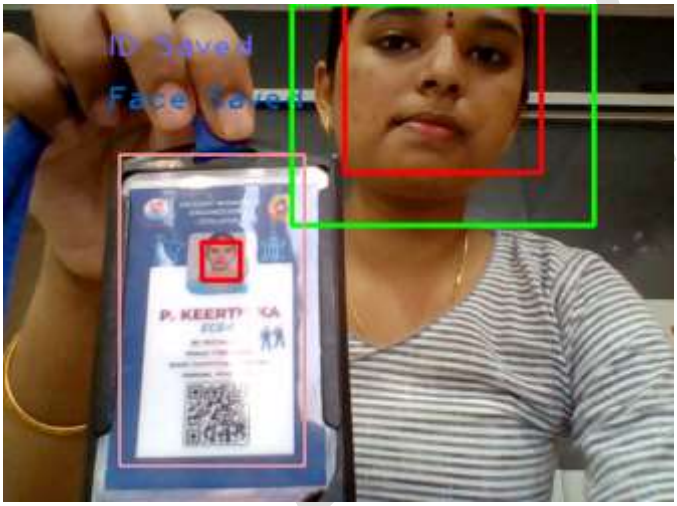


Fig.9 ID Saved

Step-4: After enrolling and saving the images, the system is ready for the verification process.

Fig.10 Welcome Message is shown as it matches the database and ID card.

Step-5: After verifying the student then the attendance is recorded in the excel sheet directly.

	A	B	C	D	E	F
1	Name	Year	Month	Day	Hour	Minute
2	P.Keerthika[19D21A04G4]	2023	5	12	23	2
3	P.Keerthika[19D21A04G4]	2023	5	12	23	3
4	P.Keerthika[19D21A04G4]	2023	5	12	23	25
5	P.Keerthika[19D21A04G4]	2023	5	12	23	26
6	P.Keerthika[19D21AO4G4]	2023	6	3	18	35
7	P.Keerthika[19D21A04G4]	2023	6	3	20	20
8						

Fig. 11 Recorded Attendance in Excel Sheet

Hence, if a student is found with his/her own id card then the system detects and records the attendance in Excel sheet.

There is also one more thing that if a student found without ID card during verification, then it shows the text that person without id card found with the bounding box around the face of that person. It also sends the email to the admin plays the audio alert message.

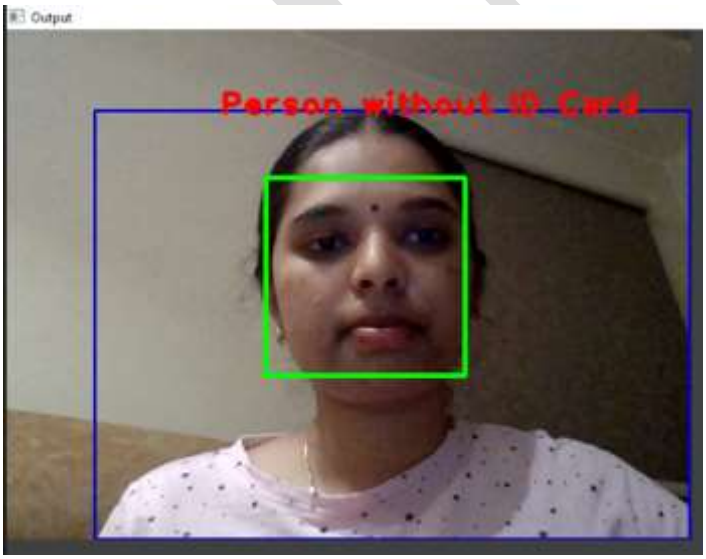


Fig.12 Person Without ID card

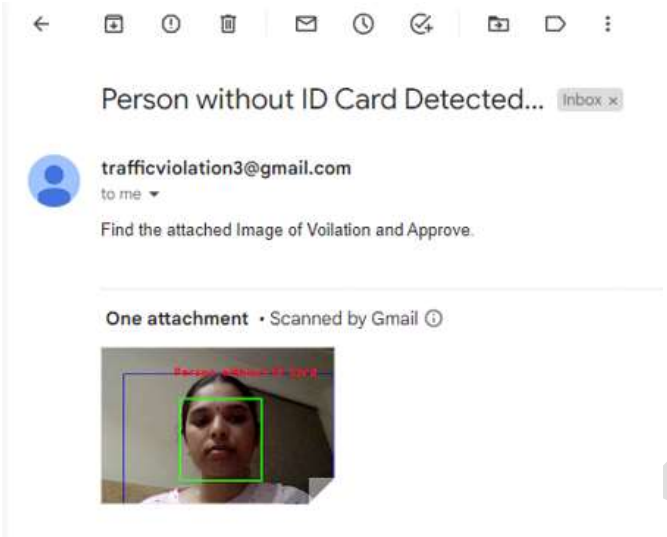


Fig. 13 Mail Sent to the Admin

Once the person got detected without ID card then the proposed work immediately sends this violation to the respective college administrator.

	Name	ImageNa	Year	Month	Day	Hour	Minute
2	Unknown	voilation	2023	4	25	19	3
3	Unknown	voilation	2023	4	25	19	3
4	Keertika[234]	voilation	2023	4	25	20	12
5	Keertika[234]	voilation	2023	4	25	20	16
6	Keertika[234]	voilation	2023	4	25	20	20

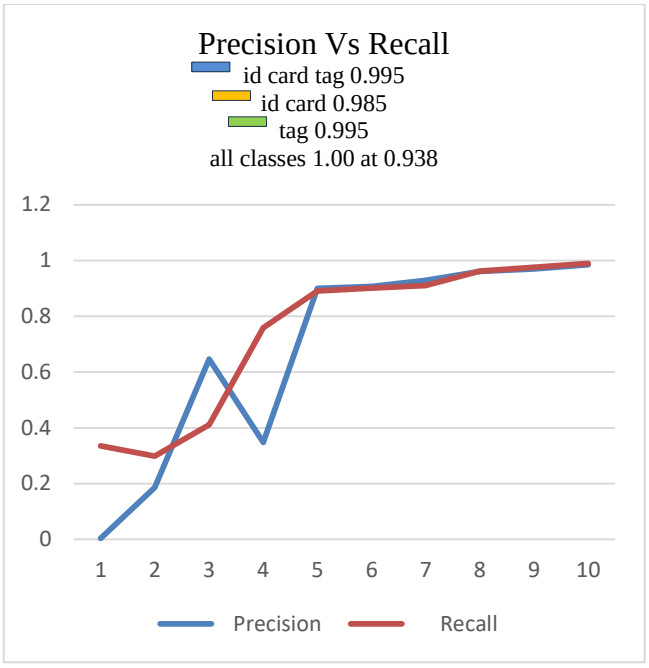
Fig.14 Details of person without ID card in Excel sheet

It also records the details of that person in excel sheet as unknown person. Fig 14 shows the output how details get recorded in the excel sheet if a person found without ID card.

Epoch	Precision	Recall
0	0.0035221	0.33541
1	0.18569	0.2984
2	0.64651	0.41105
3	0.34804	0.75866
4	0.89976	0.89056
5	0.90681	0.90056
6	0.92888	0.91076
7	0.96048	0.96235
8	0.96985	0.97532
9	0.98448	0.98909

Table.1 Precision Vs Recall

Table.1 gives the precision and recall values after performing the experiment of our proposed work. By observing this table, we got 98% accurate results.



Graph.1 Precision vs Recall

The above graph shows the precision Vs recall of our proposed work. Our work aims about 98% results.

V. CONCLUSION

For raising educational quality, educational institutions nowadays are looking for ways to incorporate new technologies. This methodology will take the place of the conventional approach as everything moves towards the most recent developments. By increasing security for educational institutions and reducing fraudulent activity, this system is efficient and successful. We have a cost-effective method. A diversified dataset of actual student photos and his or her own ID card photographs are used to conduct this procedure. We also added QR codes to each of their ID cards with the goal of boosting security. Therefore, for a chance to enter the college and be given attendance, each student should only be wearing his or her own ID.

The success of our work for student authentication is measured by the method's average accuracy, which is 98%. During the enrollment process, there is a minor problem with preserving the ID card when there are various lightning situations, which causes some accuracy to be lost. We are investigating this issue right now and preparing to expand our approach so that it will also work remarkably well under various lightning circumstances.

REFERENCES

[1] M. Schiefer, “Smart home definition and security threats,” in 2015 ninth international conference on IT security incident management & IT forensics, 2015, pp. 114–118.

[2] S. Bauk and A. Schmeink, “RFID and PPE: Concerning workers’safety solutions and cloud perspectives a reference to the Port of Bar (Montenegro),” in 2016 5th Mediterranean Conference on Embedded Computing (MECO), 2016, pp. 35–40.

[3] J. Xu, H. Gao, J. Wu, and Y. Zhang, “Improved safety management system of coal mine based on iris identification and RFID technique,” in 2015 IEEE International Conference on Computer and Communications (ICCC), 2015, pp. 260–264.

[4] S. Barra, A. Casanova, F. Narducci, and S. Ricciardi, “Ubiquitous iris recognition by means of mobile devices,” Pattern Recognit. Lett., vol.57, pp. 66–73, 2015.

[5] C. Yuan, X. Sun, and R. Lv, “Fingerprint liveness detection based on multi-scale LPQ and PCA,” China Commun., vol. 13, no. 7, pp. 60–65,2016.

[6] X. Sun, J. Shang, S. Liang, and Y. Wei, “Compositional human pose regression,” in Proceedings of the IEEE International Conference on Computer Vision, 2017, pp. 2602–2611.

[7] C. L. Witham, “Automated face recognition of rhesus macaques,” J. Neurosci. Methods, vol. 300, pp. 157–165, 2018.

[8] M. Shirodkar, V. Sinha, U. Jain, and B. Nemade, “Automated attendance management system using face recognition,” Int. J. Comput. Appl., vol. 975, p. 8887, 2015.

[9] W. Zhao and R. Chellappa, “Image-based face recognition: Issues andmethods,” Opt. Eng. York-marcel dekker Inc., vol. 78, pp. 375–402, 2002.

[10] M. Ao, D. Yi, Z. Lei, and S. Z. Li, “Face recognition at a distance: system issues,” in Handbook of Remote Biometrics, Springer, 2009, pp. 155–167.

[11] C. J. Bennett and D. Lyon, Playing the identity card: surveillance, security and identification in global perspective. Routledge, 2013.

[12] M. A. Sarrayrih and M. Ilyas, “Challenges of online exam,performances and problems for online university exam,” Int. J. Comput. Sci. Issues, vol. 10, no. 1, p. 439, 2013.

[13] S. Ravichandran, “Smart Identity Card.”

[14] I. Assadi, A. Charef, N. Belgacem, A. Nait-Ali, and T. Bensouici, "QRS complex based human identification," in 2015 IEEE International Conference on Signal and Image Processing Applications(ICSIPA), 2015, pp. 248–252.

[15] Page, Adam, Amey Kulkarni, and TinooshMohsenin. "Utilizing deep neural nets for an embedded ECG-based biometric authentication system." 2015 IEEE Biomedical Circuits and Systems Conference (BioCAS). IEEE, 2015.

[16] Kaur, Barjinder, Dinesh Singh, and ParthaPratim Roy. "A novel framework of EEG-based user identification by analyzing music- listening behavior." Multimedia tools and applications 76.24 (2017):

25581-25602.

[17] Gui, Qiong, ZhanpengJin, and Wenyao Xu. "Exploring EEG-based biometrics for user identification and authentication." 2014 IEEE Signal Processing in Medicine and Biology Symposium (SPMB). IEEE, 2014.

[18] Bailey, Kyle O., James S. Okolica, and Gilbert L. Peterson. "User identification and authentication using multi-modal behavioral biometrics." Computers & Security 43 (2014): 77-89.

[19] Bo, Cheng, et al. "Silentsense: silent user identification via touch and movement behavioral biometrics." Proceedings of the 19th annual international conference on Mobile computing & networking. ACM, 2013.

[20] Alzubaidi, Abdulaziz, and Jugal Kalita. "Authentication of smartphone users using behavioral biometrics." IEEE Communications Surveys & Tutorials 18.3 (2016): 1998-2026.

[21] W. B. Lund, D. J. Kennard, and E. K. Ringger, "Combining multiple thresholding binarization values to improve OCR output," in Document Recognition and Retrieval XX, 2013, vol. 8658, p. 86580R.

[22] Y. Chemla and C. Richard, "Security device, method and system for financial transactionas, based on the identification of an individual using a biometric profile and a smart card." Google Patents, 08-Aug- 2017.

[23] Hameed, Sarmad, et al. "Radio frequency identification (RFID) based attendance & assessment system with wireless database records." Procedia-Social and Behavioral Sciences 195 (2015): 2889-2895.

[24] Zaman, Hasan U., et al. "RFID based attendance system." 2017 8th International Conference on Computing, Communication and Networking Technologies (ICCCNT). IEEE, 2017.

[25] Jackson, Daniel, Fred Bargetzi, and Brian Donlan. "User identificationand location determination in control applications." U.S. Patent No. 9,602,172. 21 Mar. 2017.

[26] Koppikar, Unnati, et al. "IoT based smart attendance monitoring system using RFID." 2019 1st International Conference on Advances in Information Technology (ICAIT). IEEE, 2019.

[27] Soumil Nitin Shah and Abdelshakour Abuzneid. "IoT Based Smart Attendance System (SAS) Using RFID" 2019 IEEE Long Island Systems, Applications and Technology Conference (LISAT). IEEE, 2019.

[28] Yazid, Asim Balarabe, et al. "Four-factors authentication algorithm for preventing fake attendance." 2019 15th International Conference on Electronics, Computer and Computation (ICECCO). IEEE, 2019.

[29] Lia Kamelia, Eki Ahmad Dzaki Hamidi, et al. "Real-Time Online Attendance System Based on Fingerprint and GPS in the Smartphone." 2018 4th International Conference on Wireless and Telematics (ICWT). IEEE, 2018.

[30] L. Kamelia, E. A. D. Hamidi, W. Darmalaksana and A. Nugraha, "RealTime Online Attendance System Based on Fingerprint and GPS in the Smartphone," 2018 4th International Conference on Wireless and Telematics (ICWT), 2018, pp. 1-4, doi: 10.1109/ICWT.2018.8527837.

[31] Vasutan Tunbunheng "Automatic Attendance System for late students using speech recognition corresponding with google forms and sheets 2017 10th International Conference on Ubi-media Computing and Workshops (UbiMedia). IEEE, 2017.

[32] B. Soewito, F. L. Gaol, E. Simanjuntak and F. E. Gunawan, "Smart mobile attendance system using voice recognition and fingerprint on smartphone," 2016 International Seminar on Intelligent Technology and Its Applications (ISITIA), 2016, pp. 175-180, doi: 10.1109/ISITIA.2016.7828654.

[33] Q. Shafi, J. Khan, N. Munir and N. K. Baloch, "Fingerprint verification over the network and its application in attendance management," 2010 International Conference on Electronics and Information Engineering, 2010, pp. V2-555-V2-559, doi: 10.1109/ICEIE.2010.5559744.

[34] Vivek, L. Rajasekar1 S. "Wireless fingerprint attendance system using ZigBee technology." International Journal of Power Control Signal and Computation (IJPCSC) Vol3. No1 (2012).

[35] Ahmedi, Aziza, and Suvarna Nandyal. "An automatic attendance system using image processing." The International Journal Of Engineering And Science (IJES) 4.11 (2015): 1-8.

[36] Sutabri, Tata, Ade Kurniawan Pamungkur, and Raymond Erz Saragih. "Automatic attendance system for university student using face recognition based on deep learning." International Journal of Machine Learning and Computing 9.5 (2019): 668-674.

[37] Wei, Xiong, et al. "QR Code Based Smart Attendance System." International Journal of Smart Business and Technology 5.1 (2017): 1-10.

[38] S. Homayon and M. Salarian, "Iris recognition for personal identification using LAMSTAR neural network," arXivPrepr. arXiv1907.12145, 2019.

[39] D. Cheng, Y. Gong, S. Zhou, J. Wang, and N. Zheng, "Person reidentification by multi-channel parts-based cnn with improved triplet loss function," in Proceedings of the iEEE conference on computer vision and pattern recognition, 2016, pp. 1335–1344.

[40] Z. Wu, Y. Huang, L. Wang, X. Wang, and T. Tan, "A comprehensive study on cross-view gait based human identification with deep cnns," IEEE Trans. Pattern Anal. Mach. Intell., vol. 39, no. 2, pp. 209–226, 2016.

[41] Y. Wen, K. Zhang, Z. Li, and Y. Qiao, "A discriminative feature learning approach for deep face recognition," in European conference on computer vision, 2016, pp. 499–515.

[42] J. Zhu, H. Ma, J. Feng, and L. Dai, "ID card number detection algorithm based on convolutional neural network," in AIP Conference Proceedings, 2018, vol. 1955, no. 1, p. 40124.

[43] N. Wang, X. Zhu, and J. Zhang, "Research of ID card recognition algorithm based on neural network pattern recognition," in 2015 International Conference on Mechatronics, Electronic, Industrial and Control Engineering (MEIC-15), 2015.