Real-Time Face and QR Code Verification System for Attendance and Access control

Dr. G. Saritha[1], D Maneesha[2], V. Bhanu[3], D. Ravichandravarma[4]

[1]Associate Professor, Department of Computer Science and Engineering, Methodist College of Engineering and Technology, Hyderabad, India.

[2]B.E. Student, Department of Artificial Intelligence and Data Science, Methodist College of Engineering and Technology, Hyderabad, India.

Abstract -

The system named as Real Time Face and QR Code Verification System for Attendance and Access Control is created in order to facilitate attendance and to provide security at the same time. The conventional attendance techniques suffer from a number of disadvantages such as cheating of one student by another, error during recording, and most importantly lack of proper security. Therefore, the conventional techniques cannot be taken as highly reliable sources. Initially, we did not have any particular reason behind the selection of this topic, but rather decided to test it out randomly. In our system, we adopted a combination approach wherein we used face detection technique and QR code scanning simultaneously. Upon the arrival of an individual, the face of the individual is detected by the camera and compared against the database of images, while QR code is read simultaneously. In case both face and QR code belong to the same person, the system will let the person pass; otherwise, it won't allow that person entry into the building. We have also incorporated face detection capability into our system, which will help it detect whether the person attempting to access the building is a live person or simply a picture/video. This feature will go some way in minimizing cheating on the part of the user. All the collected information will be stored in the database, making its management easy and convenient. Though the system is prone to certain limitations, most problems associated with the traditional method of collecting attendance have been eliminated. During the testing of the system with different individuals, it worked quite effectively for us. The system may be implemented in educational institutions and offices among other similar premises where attendance and security are concerned.

***Index Terms*—Access Control, Attendance Management, Biometric Authentication, Face Recognition, Liveness Detection, Multifactor Authentication, QR Code Verification, Real-Time Systems, Security Monitoring**

1. INTRODUCTION

Biometrics have been perceived to be secure because they rely on physical traits of an individual. Each individual has distinct physical traits that make it difficult for anyone else to forge. Face recognition has been extensively applied due to its simplicity and non-contact requirement, making it more convenient in practical settings than the traditional methods. On the other hand, the system is not entirely reliable. During our development, we identified one security risk known as spoofing where an individual can trick the system into recognizing a photograph or a video as an actual person. The system cannot distinguish between the two, leading to errors. As such, we found it less reliable for use in different scenarios. QR Code system also has several challenges. At times, individuals could share their unique QR codes with other people. Or perhaps, somebody could use it without prior consent. It was tested by us as well to determine the probability of any kind of misuse. Hence, QR code alone is also not completely safe for authentication purposes.

Thus, it was evident from all of this that merely using one kind of authentication does not suffice. That was why we used two different forms of authentication, such as face recognition and QR code. It was pretty straightforward, since we did not want to rely on just one way. Therefore, in our model, when the user approaches our system, we scan their face and read the QR code simultaneously. Then, we checked against the stored information and authenticated the user based on those two methods. If both matched, then we granted access; otherwise, we did not grant access.

Furthermore, another mechanism we have incorporated is known as the liveness test, where we check whether it is an actual human being accessing our system. While testing the system, it worked better when we used both than just either of them individually. The use of proxy attendance was minimized in many cases. It did not work perfectly all the time, but it was doing well overall… hence, we found it reliable. Moreover, this system does not have any geographical limitations. It can be used at colleges, offices, and other such institutions. It minimizes small errors made in manual attendance systems.

2. LITERATURE REVIEW

Efficient attendance and access control systems have been widely discussed recently, primarily because of the need to automate the attendance process in schools, universities, businesses, and other institutions. The present-day attendance control systems, like registers and cards, are inefficient and prone to errors, such as proxy attendance. In order to solve the problem with the existing attendance systems, the application of various biometric technologies for authentication, such as face recognition, has been proposed.

The conventional approach to creating an attendance system based on face recognition was associated with the use of traditional image processing methods and machine learning algorithms to detect a person and register their attendance. Even though the implementation of the conventional face recognition attendance system improved the performance of the process, it also faced some challenges due to external factors, such as spoofing. Thus, in order to address the limitations of the conventional approach, new techniques were suggested using CNN and deep learning methods.

In addition to biometrics-based solutions, QR code- based attendance management systems have also been deployed in bulk since they are easier to deploy. In such systems, the user has to attend by scanning a particular QR code. But then again, this sort of solution involving QR codes has a tendency of getting misused because several users can attend through the same QR code. Such misuse could possibly cause issues like that of proxy attendance. To solve this issue, a hybrid model involving QR code and face recognition technology is suggested.

As we were implementing the project, it became necessary to ensure that the system does not fall prey to photos or videos that may try to pass off as individuals. Hence, we ensured that the system verified whether the individual is physically present before processing his/her identity. For instance, the system tracks whether the individual blinks or moves slightly. The system also verifies whether the facial features being processed belong to a living person. In addition, we felt it was important to have an attendance monitoring system. Therefore, the system monitors who is accessing the system. Judging from other existing systems, most of them lack this feature.

Nonetheless, even in light of all the above innovations, it may be pointed out that the bulk of such systems have limitations, as they were either intended for the attendance purposes or security. Second, there is no integration of these two features into a single unit. Third, there is no real- time decision-making and logging in place.

This real-time face recognition and verification system, on the other hand, could address all these issues, as it includes both face recognition, QR coding, as well as live recognition technology. It provides real-time verification as attendance is registered upon successful face recognition and QR recognition.

3. SYSTEM ARCHITECTURE

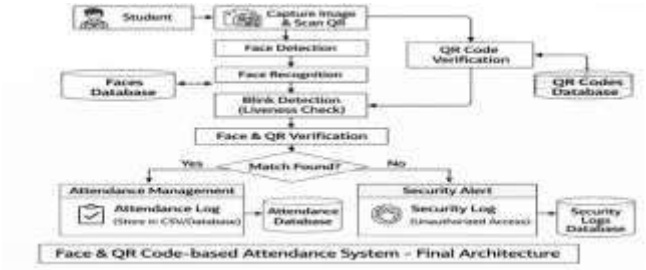

Figure.1-System Architecture of Real-Time Face and QR Code System.

The moment when the student approaches to check in, the picture of their face is taken through a camera. At the same time, a scan of the QR code is performed. The face matching system detects whether the scanned face is matched with any of the images available in the system. In case of a positive result, the person is marked as 'present'. In case of a negative result, the person is detected as not authorized and denied access. Hence, it ensures the attendance is only recorded for authorized students and not by anyone else. To avoid spoofing, another technique of liveness detection would be used for this system. In this technique, the eye blink detection system will verify whether the input data is a live individual or a video/photograph. Apart from the biometric process discussed above, the credential validation layer also consists of the process of validation of QR codes. For this purpose, the QR code generated by the individual is scanned and validated using the already existing database of QR codes.

The decision-making and fusion layer forms the core component of this system. The output from the face recognition layer, the liveness detection layer, and the QR code validation layer is included here. When a student visits the class to register for attendance, the camera captures the image of the face. This system also verifies if the student blinks. In this way, it confirms that the person standing in front of the camera is a live human and not an image. While capturing the image of the face,

it also scans the QR code of the student. Only after verifying the two elements – the image of the face and the QR code – can the student access the classroom. While testing the system, it performed well with both registered and non-registered students. It was very clear to understand how the system was working. All that it did was display messages. For example, whenever the student was authorized, it displayed "Access Granted," and in case he or she was not registered, it displayed "Unknown User." Additionally, the system worked very fast. It was very hard to find any lagging, even during testing with multiple students accessing at the same time.

4. IMPLEMENTATION

There was no proper procedure followed during the check. Only attempts were made this way just for understanding the process. There was one student standing in front of the camera while we observed the whole thing. Suddenly, there started the whole process from their side. It was doing the facial recognition along with scanning the QR code at the same time. Then it will match the information with the one already fed into it. First of all, we did not understand it well, but later after observing it 2-3 times, we got a clear picture about it. Only when there was a match between the facial recognition and the QR code of the same individual that his/her presence would be recognized.

As far as the testing environment goes, there were changes; light was too strong at times, too little at others, or there was a shadow falling over the face. Nevertheless, this did not affect the overall performance; the system mostly operated well…mostly. The testing was also conducted on people who were not enrolled in the system; nevertheless, the system refused to work. Testing was not done in one way or another; sometimes, students moved, and the QR code was not quite visible. Nevertheless, the system tried its best to identify the person. On some occasions, this was achieved; on other occasions, the result was negative; which is fine. The tests were also done using QR codes before faces were scanned.

All the components were built using Python. The camera operation is performed using OpenCV module. For the identification process, face recognition and dlib are utilized. For the graphical user interface development, Tkinter is employed since it makes things easy. Each component performs a particular function on its own, nothing too complex but altogether functioning.

Initially, the students should be registered. Their facial images and QR codes are captured and stored. Subsequently, when they visit the class, system captures the facial image and the QR code and validates their identity. In case their identification proves successful, attendance record is updated containing their names and date along with timestamp. On the other hand, the system will block access and records details of the failed attempt in log file. Everything is quite straightforward; each component works independently giving results and making system decide whether it will allow or deny access. In case all the components show good results, the student gains access else denied. Student just needs to place his QR code before the system and it will do all other things automatically. We realized that it can be further improved in future. This could include storing data online or using mobile also.

5. METHODOLOGY

When the system was first tested, no preparations had been made at all. The system simply called upon a student to be in front of the camera and see what would happen. During that period, the system was actually capturing the face photo and reading the QR code at the same time. Based on what we observed, the system only checked on the face since the background had little to no effect on the process. Afterwards, the system checks its records with the existing data previously captured. Attendance is noted when there's a match between the face and QR code in relation to the particular student.

However, when we were testing, we were not always in similar conditions. At times, light used to be excess, at times it used to be insufficient, and at times there used to be shadows falling on the face. This was causing some change in the results. However, despite all this, most of the times the system was recognizing successfully.

There was also an experiment where we gave images of people who are not registered in the database, and there also, the system restricted their access with an appropriate message. It wasn't like we tested with only one method. At times, some of the students used to move slightly even while standing, and also the QR image used to be unclear.

After going through all this, it feels that it is possible to implement it in practical scenarios as well. It may not be foolproof in all conditions, but yet it performs quite satisfactorily. In simpler terms, once a student arrives, the system first scans the face and then scans the QR code.

It then verifies this information against the stored database and also confirms whether it is an actual student or just a picture of the same. Once verified, it marks attendance with the details of the name, date, and time of arrival.

6. RESULTS

1. User Interface

Figure:1:User Interface

This is the main menu of the system. This system was created with the help of Tkinter. This is the menu from where all options are available. The user is provided with the freedom to select an option.

2. Student Registration

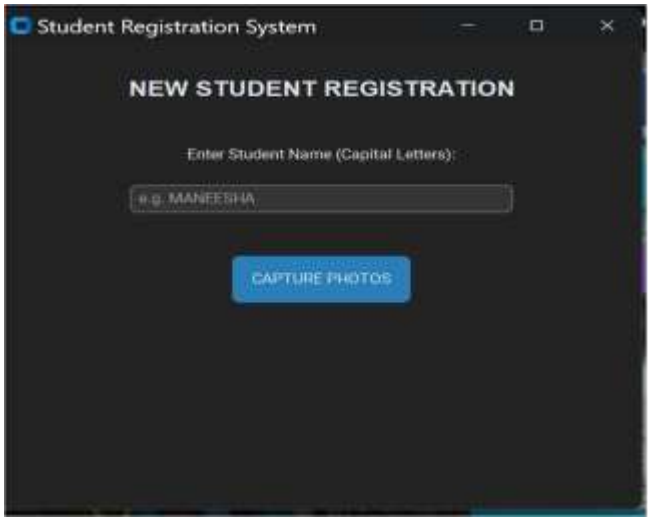

Figure:3:Student Registration

For a new user, the system uses the name and then scans the face images. The images get stored. Then when the same user arrives later, the system will recognize him. We did so just for checking purpose.

3. Attendance Logs

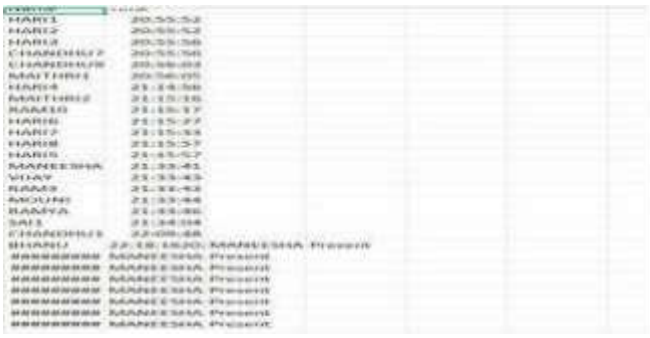

Figure:3:Attendence Logs CSV File

Attendance details can be seen in another window. Attendance shows the name and time. The data can be saved into CSV file. This makes it possible to check later if required.

4. Liveliness Detection

Figure:4:Liveliness Detection

There is another step at which system checks the authenticity of face. It detects eye blinking. In case there is no activity, it may reject face. This way it prevents any false authentication.

5. Access Granted

Figure:5:Access Granted

There is another section as well. Both face and QR code are verified in that section. Only if both of them are verified ,the system allows.

7. CONCLUSION

We focused on developing this system primarily to facilitate attendance and prevent any false inputs. Rather than implementing one type of authentication, we decided to use facial recognition and QR Code so that they cannot be easily manipulated. During testing we realized that the software can authenticate using both, making it easy to prevent any malicious activities. One interesting aspect of this project was that it produces results instantly, thus giving a feeling of speediness. Furthermore, all our components were properly aligned so that there were no problems during operation.

Moreover, we came up with a tracking mechanism to record whatever takes place in the process. In case anything goes wrong, the error is logged in for future analysis purposes. Our analysis showed that, in most cases, the program is running smoothly and delivering accurate results based on the input data. At the beginning stages of my test, I needed to see if the software will perform correctly in actual circumstances. To do this, I invited several college students to give it a go. I had some students who were already listed in the system, some who were not, and even some with fictional codes. I observed closely and found it quite intriguing to find that the software flagged the appropriate candidates only and did not recognize the other.

I tested the system in various rooms. Some had very bright lights. Others had moderate lighting. There were also those with dim lighting. During the testing process, I realized that the system would still work efficiently despite the varying conditions of lightings. There could have been situations where the illumination was a bit too bright or dimmed down, yet it still worked efficiently. As a result, I realized that it could be implemented in actual environments and was not just limited to a controlled environment.

In conclusion, I believe that this technology could be applied in institutions such as educational centers or workplaces. In the future, it would be possible to store information in the cloud, hence making it accessible from any place. It would also be possible to develop an application for users to view their attendance record. Through this project, I learned many practical things about developing software applications.

8. FUTURE SCOPE

Some ideas popped up during this work. Attendance saving on the cloud looks much better than on paper – nothing will get lost and will be available at any time. Also, there might be an application with a user-friendly interface where students will be able to check their own attendance, QR codes can also have their security improved somehow. There were several issues when I was testing the system. Face recognition stopped working properly in case of excessive illumination or in very dimly-lit conditions. Perhaps, other approaches can be developed.

Voice recognition or fingerprint scanning might be added as extra security measures. It can interact with door locks and other mechanisms too. In some cases it was operating incorrectly, therefore, providing a notification might be helpful. The question of using the gathered data is quite sensitive; I suppose that the data shouldn't be shared and, if possible, training might be conducted without transferring it elsewhere.

REFERENCES

[1] A. Kumar et al., "EagleAI: Real-Time Restricted Area Surveillance System," 2025.

[2] S. Reddy et al., "Facial Recognition- Based Attendance Monitoring System," 2025.

[3] P. Sharma et al., "Contactless Smart Attendance System Using Face Recognition and QR Code," 2024.

[4] R. Gupta et al., "Surveillance System with Human Intrusion Detection," 2024.

[5] M. Verma et al., "Real-Time Face Tracking for Attendance Monitoring," 2025.

[6] K. Singh et al., "Lightweight Face Recognition with Liveness Detection," 2024.

[7] D. Patel et al., "QR Code-Based Attendance System," 2025.

[8] T. Rao et al., "Multi-Sensor Surveillance System for Threat Detection," 2024.

[9] N. Das et al., "Smart CCTV with Visitor Management and Face Detection," 2023.

[10] V. Mehta et al., "YOLOv8-Based Anomaly Detection in Restricted Zones," 2024.

[11] A. Bose et al., "Hybrid Face and Voice Authentication System," 2024.

[12] L. Chen et al., "Deep FaceNet for Access Control Systems," 2025.

[13] H. Ali et al., "Cloud-Based Face Recognition Attendance System," 2023.

[14] S. Iyer et al., "YOLOv7 Intruder Detection System," 2023.

[15] J. Wang et al., "Federated Learning for Face Recognition Systems," 2024.

[16] R. Sharma et al., "Blockchain-Secured QR Code Attendance System," 2025.

[17] P. Nair et al., "Motion-Based Liveness Detection Using Deep Learning," 2024.

[18] K. Lee et al., "Edge-Based Surveillance Analytics Using AI," 2023.

[19] Y. Zhang et al., "Multi-Modal Surveillance Fusion for Threat Detection," 2025