ijamrsd.com
ISSN: 2583-6404
Journal of Advanced Multidisciplinary Research Studies and Development
Peer Reviewed Referred Journal | Bi-monthly | Open Access

SECURE AUTHENTICATION FRAMEWORK USING SECURE QR CODE AND FACE RECOGNITION FOR CONTROLLED ACCESS AND EXAMINATION INTEGRITY

Aniket Dilip Bhujbal[1], Vaishnavi Sudesh Parit[2], Anjali Naik[3], Vrushali Limaye[4]
[1] *Department of Mathematics, Fergusson College (Autonomous) Pune.*
Email: aniketsocialmail@gmail.com
[2] *Department of Mathematics, Fergusson College (Autonomous) Pune.*
Email: vaishnaviparit712@gmail.com
[3] *DES, Institute of Management Development and Research, Pune.*
Email: anjali.naik@imdr.edu
ORCID: 0009-0006-1713-8198
[4] *Department of Mathematics, Fergusson College (Autonomous) Pune.*
Email: vrushali.limaye@fergusson.edu
ORCID: 0009-0006-5564-3128

Abstract
The digital transformation has radically changed the educational, organizational and professional contexts. Digital transformation has significantly impacted educational, organizational, and professional contexts. Consequently, online and hybrid examinations, virtual interviews, and digital access control systems are increasingly adopted due to their scalability and user-friendliness.However, these instruments have also generated a number of security issues, among which identity verification, impersonation, proxy participation, and generally, unauthorized access, are included. Traditional authentication methods (like login and password, one-time password, or static access link) cannot recognize users physical presence and real identity.The mentioned loopholes are, to a large extent, the problem of examination environments where fairness and honesty are of utmost importance. The presence of proxy contestants, distributed URLs, and external breaches are the reasons that digital testing is less trustworthy. Furthermore, QR codes are often selected due to their simplicity and ease of access. Nevertheless, fixed QR codes can be recreated without the user's knowledge, promoted without their consent. Face recognition is an accurate biometric that can be tricked if there are no other additional contextual constraints. This paper presents a new multifactor user verification system that combines facial recognition, programmatically generates QR codes, and network-level verification to enhance security and user privacy in access control. According to the protocol, only the people who are authorized and physically present at a certain place can be given access to confidential resources such as examinations.

Keywords: Access Control, Computer Vision, Face Recognition, Examination Authentication, Privacy Preservation, QR Code Security.

► *Corresponding Author: Aniket Dilip Bhujbal*

1. Introduction

The Quick Response code has quietly entered into our modern lives while evolving from a simple marketing tool into a powerful player in the digital world. While we often hear about the danger associated with these codes, it is very interesting how these unassumingly black and white squares are being actively engineered to protect us. The value of the QR code lies in its ability to establish a fast, reliable and non-repudiable link between user and digital devices, eliminating the need for manual data entry. (Alsuhibany, 2025) [1]

A QR code is a Two-dimensional (2D) matrix barcode designed to store information that allows quickly reading using a smartphone camera. The term "QR" stands for Quick Response, reflecting its speed and efficiency in decoding information. Visually, a QR code is a pattern of black squares on a white background. It can hold different types of data, including text, website links, and digital information. QR code usage has significantly increased globally, primarily due to the widespread availability of smartphones equipped with built-in cameras. This has made scanning Quick Response codes a simple and convenient task for everyday users.First introduced in 1994, Quick Response codes were initially developed by Denso Wave, a Toyota Group subsidiary, for inventory tracking in automobile parts manufacturing. Initially intended for industrial use, QR codes have since diversified their applications.Today, QR codes are widely used in logistics, retail product labelling, marketing, entertainment, and various other digital services. By scanning a QR code, users can directly access a website, view text, or retrieve other digital content.Furthermore, these QR codes are now easily created and printed using online generators or mobile applications, making it convenient for individuals and organizations to share information effectively. The QR code system operates through two main components: an encoder and a decoder.

The encoder converts input data, such as text or URLs, into a QR code image. The decoder, usually a scanner application, reads the decodes and extracts the embedded information.(Tiwari, 2016) [2].

QR codes can be either static or dynamic. A static QR code cannot be modified after generation, while a dynamic QR code allows for updates.

One of the most powerful applications of this Quick Response code is in document authentication. Nowadays more and more institutions are embedding secure, digitally signed QR codes onto official documents like academic transcripts and certificates. This permits anyone with a smartphone to instantly verify the document's authenticity. (Pandiri & Varshney, 2024) [3]

2. Objectives

The key objectives of this research are

A) Secure and well-founded authentication system with the help of QR codes combined with facial recognition.

The key objective of the research is to design and apply a safe and working authentication system by integrating dynamic QR code technique with face recognition-based verification. The system also aims to overcome the limits of conventional mechanisms, such as login credentials and passwords, which are weak and easy to exploit and share.

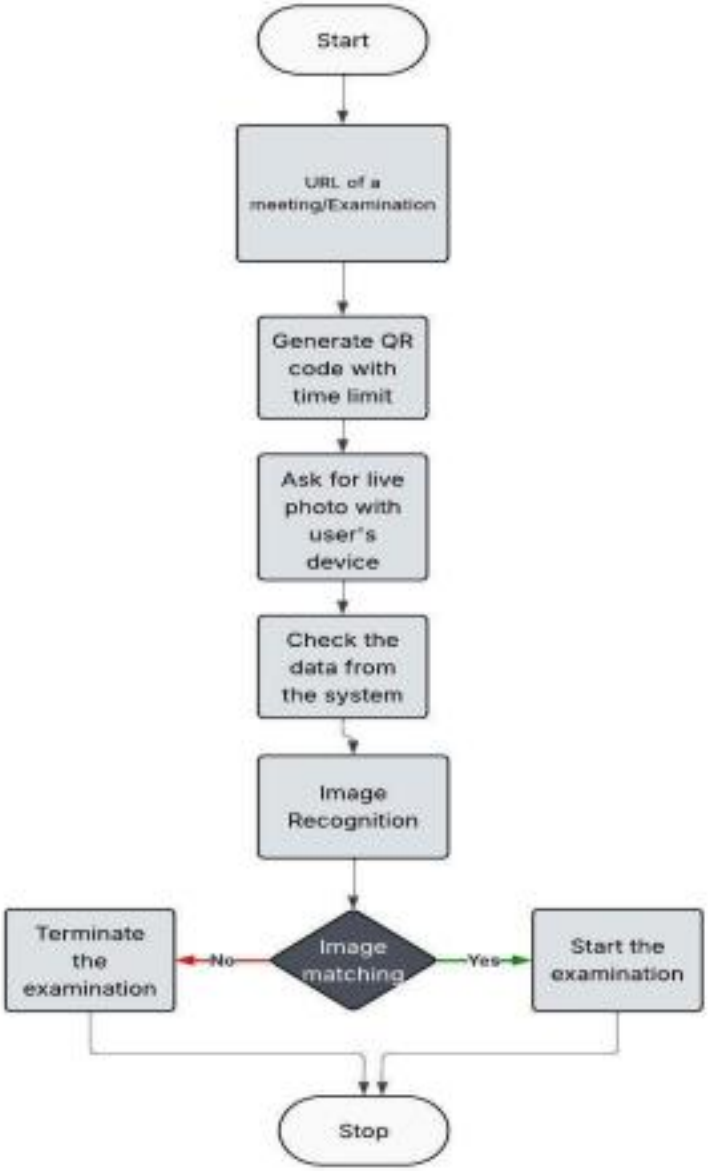
B) Identity verification is a security step to confirm that the user taking a test is actually a registered individual and not someone impersonating while ensuring fair results and forthrightness. [pretending to be them (impersonation), guaranteeing fair results and preventing cheating.] (Wang et al., 2024) [4] Here, we aim to identify verification and ensure the test appeared by the rightful individual, avoiding malpractices and maintaining fairness and honesty in the assessment process.

C) While using the system, the system mandates that both the verification server as well as the user function on the same Wi-Fi network, ensuring a controlled set that avoids irregular access and verification contradictions.
D) This code is executed in python with the integration of Artificial Intelligence and computer vision /python libraries for the generation of QR codes, face recognition, and real date and time.(Wahsheh,2021)[11] The system uses, Python as the programming language, AI and computer vision techniques. Also, libraries for QR code generation, facial recognition, and real-time date and time processing are used. (Wang et al., 2024) [4]
E) Implementing a system that securely records images of applicants. The system verifies the image every time even if the user provides the same images repeatedly.
Each time the applicants verify their image, the system must securely record the images as a compulsory step.
F) Ensures that the data given by the individual is used ethically with the user consent.

3. Code Flow-For and Flow Chart

Table No 1: System Working Flow

Link of examination
Generation of QR code within time limit
Ask for live photo from user current device
Checks the data of images from the System.
If the image is recognized successfully, access is granted otherwise, the image is saved to the admin and access is denied
Start the test



4. Methodology

4.1 Overview of the Proposed Framework

The suggested framework's first application is a multilevel authentication system. The core of security, identity verification, demonstration of physical presence, and secure access are combined with the highest technological standards. The failure of any one of these instances to meet the required level in the security layers, which are independent stages, is one of the main features of the framework.

The elements which are in charge of the system's working are: Dynamic QR code generation Time-based QR validation Network-based access restriction Facial recognition and verification Image logging for monitoring and auditing

4.2 Dynamic QR Code Generation

The person who performs authentication is an authorized administrator or a teacher, who will

initiate the safe access by giving a verified link like a school examination URL. After that, a dynamic QR code with the encrypted session information such as access link, session identifier, and timestamp is generated by the system.

The QR code is allotted a time-to-live (TTL) which varies from two to five minutes. Once the QR code has expired, it automatically becomes invalid thus eliminating any reuse or time-delayed access. This dynamic behavior is one of the ways by which the risk of sharing QR codes is greatly reduced. (Suresh, 2023)[6]

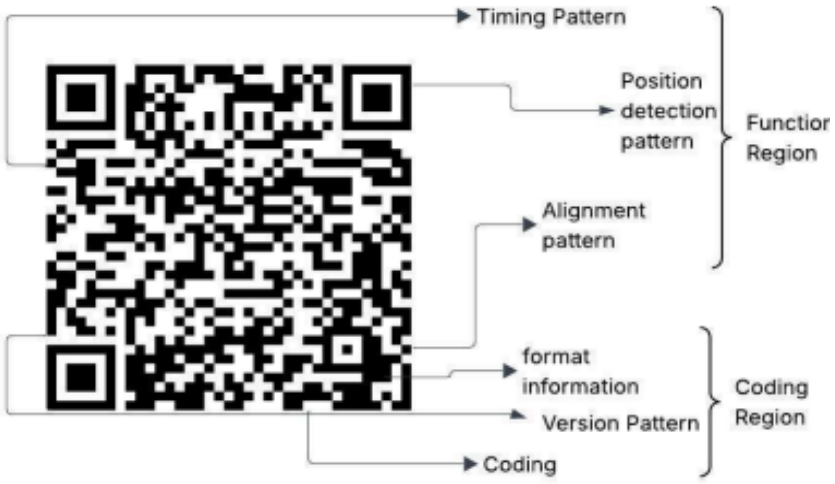


Figure No 1-Structure of QR code.

A QR code constructs several functional and coding regions that work together to store and to fetch the data successfully as shown in Fig. 1:

● **Functional region:** It carries patterns that help scanners recognize and align the code. Position detection patterns (3 corner squares) permit quick location and direction.

Alignment patterns (smaller inner squares) correct for distortion in larger QR versions. Timing patterns (alternating dots) define the cell size and grid layout as per the QR code.

● **Coding region:** It keeps the actual data and metadata.

Format information, in a QR code, stores the error-correction level and mask pattern used for decoding.

Version information indicates the QR size (1–40), which decides the volume of the data. Data cells (the black/white cells) encrypt the user's information (text, URL, etc.) with Reed-Solomon error correction.

The combination of these patterns helps QR codes to be scanned reliably even when patterns are hidden or there is some kind of noise, even if QR code is scanned partially then also it will retrieve the data. (Huang,2020) [5]

4.3 Network-Based Access Restriction

The system examines the network connection to ascertain the user's location beyond any doubt. Access will be granted to the user only if their device is connected to the same local Wi-Fi network as that of the administrator's system. (Satanasaowapak ,2021) [16]

The mobile devices on which the request is made will be using data or will be connected to the external networks. Therefore, access will be automatically denied. The mechanism is intended not

only to guarantee the user's physical presence without requiring extra hardware but also to stop remote access. *(Tiwari et al., 2024)* [7]

4.4 Facial Image Capture and Recognition

Once the network and QR have been verified successfully, a live picture of the face has to be taken by the end user via their device's camera. Image preprocessing by detection, alignment, and normalization of the face is the next step.

Computer vision models figure out the features on the face in the image, and after that, the matching is done to find the features with the highest similarity in the registered facial data. The authentication mechanism is carried out through a certain similarity threshold. Only verified users can access the secure resource. (Abusham et al. ,2023) [12]

Figure No 2- Face Identification Concept

The image depicts a schematic facial recognition (Face ID):

1. Face detection framework: The green bounding brackets represent the region of interest (ROI) that isolates the facial area for preprocessing and analysis.
2. Facial landmark annotation: The red fiducial points mark anatomical landmarks (eye corners, nose tip, lip boundaries, jawline, etc.). These landmarks are used to construct a geometric facial model for feature extraction and alignment.
3. In face recognition, features such as eigenfaces or deep learning–based embeddings are obtained from the facial landmark data. These features are finally matched with the stored records to verify the authenticity or identify the person.

4.5 Implementation Environment and Tools

The system to be implemented is a Python-based solution. This Computer language was chosen for its flexibility and also for the AI and security-related applications that it supports extensively. The libraries that are listed below are the ones that are being utilized:

OpenCV (cv2) is used in Face detection and image preprocessing. It performs matrix operations and numerical computations using python library NumPy. This is a CNN-based model which is used for feature extraction and matching QR code. (Odeh & Odeh, 2024) [14]

HandlingOs library performs the expiry of a Quick Response code within a given time limit and Networking libraries for Network validation and system control. (Yeşiltepe et al. ,2025)[9]

DeepFace is for face recognition. We have used python library deepface 0.0.96, this library checks that the two facial images belong to the same person or to different persons. This application helped

us to separate out the authorized applicant and unauthorized applicants who are accessing the provided URL. (Deineko et al., 2022)
[8] (Kishore et al., 2025) [10]

Fig. 3. Working of DeepFace

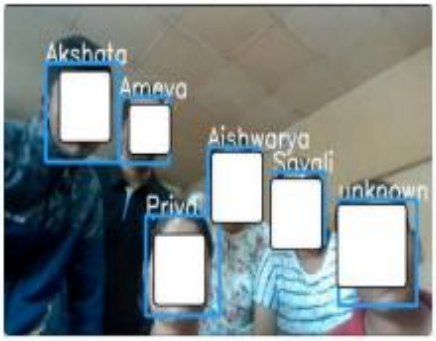


Fig. 4. Working of DeepFace

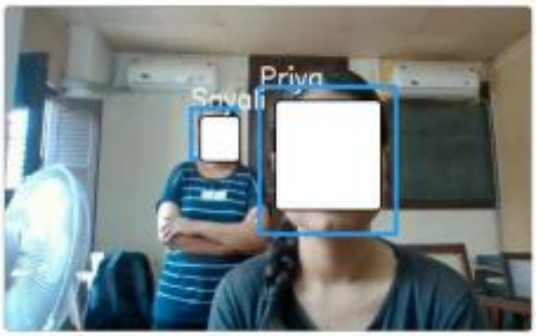


Fig. 5. Working of DeepFace

Fig. 6. Working of DeepFace

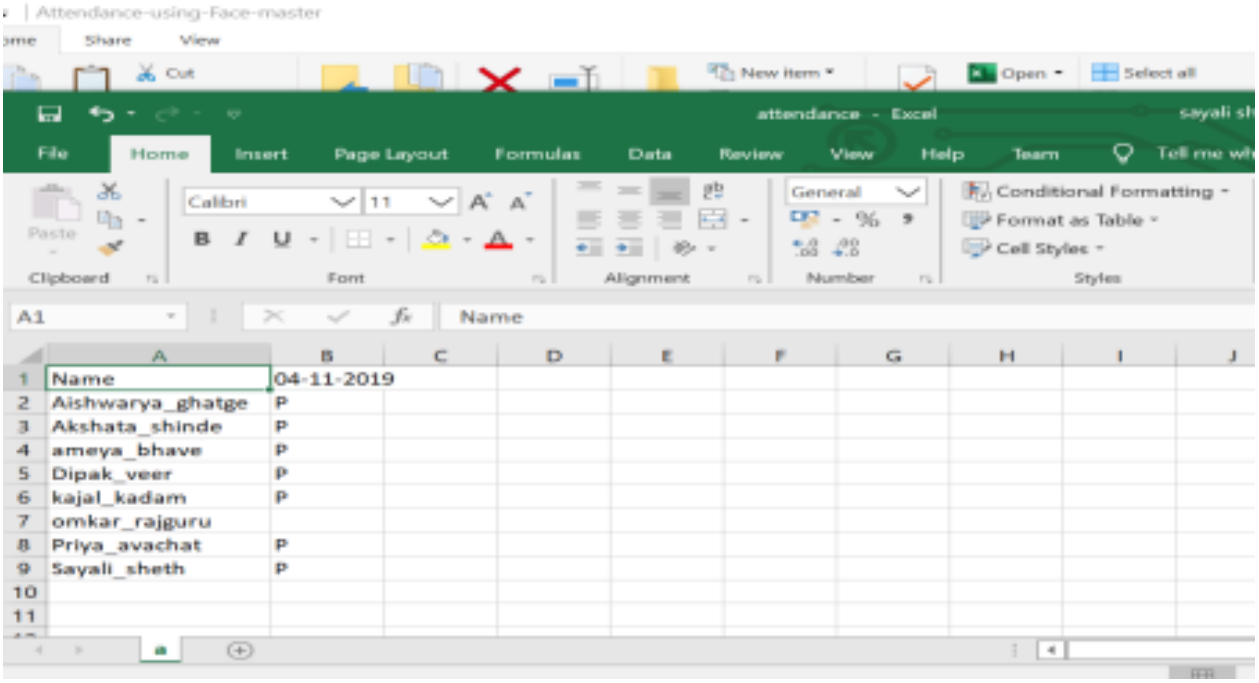


Fig. 7. Working of DeepFace

How Application Works

1. It calculates the distance.
2. It stores the data as a dictionary (key-value pair). Key is an aspect as a file name as shown in the Figure No 2- Face Identification Concept.
3. Compares the distance with the target image (below Table No II - FaceNet Embedding Distance Analysis):

Table No II - FaceNet Embedding Distance Analysis

Distance Value Meaning
I. 0.00-0.30 Match I. Very Strong
II. 0.00-0.45 II. Good Match
III. 0.45-0.60 (Threshold region) III. Can't Say
IV. >0.60 person IV. Not same

Component-based architectural design makes the system very flexible for any future planning of further development or enhancement of the system. (Schroff et al., 2015) [13]

4.6 Image Logging and Malpractice Monitoring

The image logging component integrated within the authentication flow is a crucial part of the current research. The photo of the face of the user after successful authentication will be taken along with the information on time and session ID and then stored securely.

In the case of an unauthorized access attempt, e.g., a QR code is being scanned at a place where the authorized network is not available, or facial recognition is failing; the system takes the intruder's image and saves it separately. Therefore, it can be considered as the visual evidence provided to the administrators to locate and verify the instances of the malpractice.

So, a tool is given to teachers which not only makes it easier for them to monitor security violators but also allows them to perform post-event auditing that can then be used to expose the infringements and identify those who violate the established regulations. *(Păvăloaia & Husac, 2023)* [15]

Conclusion

We introduced a multilayered privacy-conscious use for authentication system combining dynamic QR codes, face recognition, and network-based access control as part of our research. A secure system ensuring user identity authentication and exam integrity was developed in Python using AI-powered computer vision techniques. To ensure honesty and the presence of officials, image logging was implemented, making the system an ideal solution for high-risk digital environments.

Future Scope

Future work will focus on making these changes optional with the addition of liveness detection, blockchain-supported audit trails, federated learning for privacy protection, and cloud-based deployment.

References

1. Alsuhibany, S. A. (2025). Innovative QR code system for tamper-proof generation and fraud-resistant verification. *Sensors*, *25*(13), 3855.
https://pubmed.ncbi.nlm.nih.gov/40648115/ .
2. Tiwari, S. (2016, December). An introduction to QR code technology. In 2016 international conference on information technology (ICIT) (pp. 39-44). IEEE.
https://researchr.org/publication/Tiwari16-0
3. Pandiri, N. R., & Varshney, G. (2024). E-Authentication System with QR Code (EasyChair Preprint No. 12842). EasyChair. https://easychair.org/publications/preprint/tkmQ
4. Wang, R., Huang, L., Madden, K., & Wang, C. (2024, May). Enhancing qr code system security by verifying the scanner's gripping hand biometric. In *Proceedings of the 17th ACM Conference on Security and Privacy in Wireless and Mobile Networks* (pp. 42-53).
https://dl.acm.org/doi/abs/10.1145/3643833.3656128
5. Huang, J., Li, L., Wang, X., Lu, B., & Liu, Y. (2020). Recognition of distorted QR codes with one missing position detection pattern. *IET Image Processing*, *14*(13), 3154-3160.
https://doi.org/10.1049/iet-ipr.2019.1095
6. Suresh, P., Sadhya, D., & Rajput, A. S. (2023, December). Generation of Multi-Layered QR Codes with Efficient Compression. In *International Conference on Pattern Recognition and Machine Intelligence* (pp. 301-311). Cham: Springer Nature Switzerland.
https://doi.org/10.1007/978-3-031-45170-6_31
7. Tiwari, S., Üyüklü, C., & Dalkılıç, G. (2024). QR code-based authentication in IoT mesh network. In Proceedings of the 2024 8th International Artificial Intelligence and Data Processing Symposium (IDAP 2024) (pp. xx–xx). IEEE.
https://www.researchgate.net/publication/384979938_QR_Code-Based_Authentication_in_IoT_Mesh_Network
8. Deineko Zh. QR Code as an Element of Educational Activity / Zh. Deineko, N. Kraievska, V. Lyashenko // International Journal of Academic Information Systems Research (IJAISR). – 2022. – Vol. 6(4). – pp. 26-31
https://openarchive.nure.ua/handle/document/20230
9. Yeşiltepe, M., Kurulay, M., Bennour, A., Rasheed, J., & Alsubai, S. (2025). Enhancing QR code security: Exploiting hidden message mechanisms and machine learning classification. *Intelligent Decision Technologies*, *19*(2), 630-644.
https://doi.org/10.1177/18724981241302039
10. Kishore, S., Padmavathi, H. G., Sowmyshree, C. S., & Manjula, K. B. (2025). Evaluation of deep learning methods in face recognition: Datasets, metrics, and results. International Journal on Science and Technology, 16(4).
https://doi.org/10.71097/IJSAT.v16.i4.9116
11. Wahsheh, H. A., & Al-Zahrani, M. S. (2021). Secure real-time computational intelligence system against malicious QR code links. *International Journal of Computers Communications & Control*, *16*(3).
https://doi.org/10.15837/ijccc.2021.3.4186
12. Abusham, E., Ibrahim, B., Zia, K., & Rehman, M. (2023). Facial image encryption for secure face recognition system. *Electronics*, *12*(3), 774.
https://doi.org/10.3390/electronics12030774
13. Schroff, F., Kalenichenko, D., & Philbin, J. (2015). FaceNet: A unified embedding for face recognition and clustering. In Proceedings of the IEEE Conference on Computer Vision and

Pattern Recognition (CVPR 2015) (pp. 815–823).
IEEE. https://doi.org/10.1109/CVPR.2015.7298682
14. Odeh, A., & Odeh, N. (2024). OpenCV and its applications in artificial intelligent systems. In **Y. Jararweh, M. Alsmirat, M. Aloqaily, & H. B. Salameh (Eds.), Proceedings of the 2024 International Conference on Intelligent Computing, Communication, Networking and Services (ICCNS 2024) (pp. 242–249). Institute of Electrical and Electronics Engineers.
https://doi.org/10.1109/ICCNS62192.2024.10776047
15. Păvăloaia, V.-D., & Husac, G. (2023). Tracking unauthorized access using machine learning and PCA for face recognition developments. Information, 14(1), 25.
https://doi.org/10.3390/info14010025
16. Satanasaowapak, P., Kawseewai, W., Promlee, S., & Vilamat, A. (2021). Residential access control system using QR code and the IoT. *International Journal of Electrical and Computer Engineering (IJECE)*, *11*(4), 3267.
https://pdfs.semanticscholar.org/8c31/7c9c57841cc4db096e6f22649f45d34360e3.pdf