https://doi.org/10.48047/AFJBS.8.10.2026.51-73

African Journal of Biological Sciences

Journal homepage: http://www.afjbs.com

Research Paper Open Access

A ROBUST IOT-BASED FACE RECOGNITION ATTENDANCE SYSTEM WITH LIVENESS DETECTION AND ADAPTIVE LOW-LIGHT ENHANCEMENT

Mr. Anirban Majumder[a,] *,Prof (Dr.) Jhunu Debbarma[b], Prof (Dr.) Gitanjali Saha[c], Prof (Dr.) Shimal Das[d]

a. Student, Department of Computer Science & Engineering, Tripura Institute of Technology, Narsingarh, Agartala
b,d. Professor, Department of Computer Science & Engineering, Tripura Institute of Technology, Narsingarh, Agartala (jhunudb@gmail.com, shimalcs.tit@gmail.com)
c. Professor, Department of Electrical Engineering, Tripura Institute of Technology, Narsingarh, Agartala (gitanjalitit@gmail.com)

* Corresponding author: anirbanmj999@gmail.com

Volume 8, Issue 10, Oct 2026
Received: 20 July 2026
Accepted: 15 Sep 2026
Published: 27 Oct 2026
doi:10.48047/AFJBS.8.10.2026.51-73

Abstract

The main goal of this study was to create an IoT-based face recognition attendance system to improve security, automation and performance in real time environments. This system combines face recognition with liveness detection methods such as blink detection and head movement verification to reduce spoofing attempts using printed photos and static images.

To improve performance in low light, we used contrast-limited adaptive histogram equalization (CLAHE) as a pre-processing method. These improvements boost facial exposure and increase the recognition accuracy in dark conditions. The system integrates an ESP8266 IoT module and a PIR motion sensor to automate the recognition process. Instead of continuously processing the video frames, our system activates only when motion is detected which reduces the unnecessary computation and improves the energy use. Once activated the system performs real-time face recognition, automatically records attendance and prevents duplicate entries through anti-spam method. According to experimental observations the system functions dependably in a variety of real-world scenarios and lighting circumstances. The suggested method provides an automatic attendance management system for companies and schools that is safe, scalable and affordable.

Keywords: Liveness Detection; CLAHE; Anti-Spoofing; Low-Light Enhancement; PIR Sensor; Attendance Automation;

1. Introduction

Traditional attendance systems are often slow and can be easily manipulated making them unreliable in many real-world situations [7], [24]. With the rapid growth of Artificial Intelligence (AI) and Internet of Things (IoT) automated systems are increasingly used for real-time monitoring and security applications. Among the various biometric techniques face recognition offers a contactless and efficient way to verify identity [1],[39]. However, many face recognition attendance-based systems still face several challenges. These include lower recognition accuracy in low-light conditions, vulnerability to spoofing attacks using printed photos or videos and the lack of efficient real-time automation[48], [40]. Furthermore, uninterrupted video processing raises computational load and energy use. To address these issues, this work offers a strong IoT-based attendance system with several advanced techniques. The system uses deep learning-based face recognition for accurate identification along with liveness detection methods such as eye blinking and head movement verification to stop spoofing attempts. To boost performance in low lighting an adaptive image enhancement method based on Contrast Limited Adaptive Histogram Equalization (CLAHE) is applied before recognition. Moreover, the system includes an ESP8266 IoT module and a PIR motion sensor to allow the automated operation. Instead of continuously processing video frames the system activates only when the motion gets detected &it reduces unnecessary computation and improves the energy efficiency. An anti-spam feature is also implemented to prevent duplicate attendance entries. By linking these components, this system improves the recognition accuracy, promotes security and enables efficient real-time operation. These advancements make it suitable for installing in schools, offices and other practical settings.

Table 1.

2. Literature Review

2.1. *Face recognition-based attendance system*

According to the study *"Face Recognition Based Attendance Monitoring System"* (Chintalapati and Raghunadh, 2013) by recognizing people using the facial traits that are detected by the camera the face recognition technology can automatically record the attendance [10]. For facial verification the traditional methods mainly depend on feature extraction methods like Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA) and Support Vector Machines (SVM) [23]. These techniques have performed well in controlled ecosystem but when the illumination or the lighting effect, body posture and different facial expressions and due to that the accuracy of the recognition got declined.

However, the performance of the suggested system decreased under low lighting because it was mainly designed for controlling the indoor lighting environments. Moreover, there wasn't any way for the algorithm to verify whether the detected face was from a printed photograph or it is a real person. These restrictions have encouraged in the development of this advanced and secure attendance system.

2.2 *Deep learning-based face recognition systems*

Schroff et al. (2015) introduced FaceNet, a deep learning-based facial recognition model that generates highly distinguished facial embeddings. For facial verification the traditional methods mainly depend in the feature extraction methods like Principal Component Analysis (PCA), Linear Discriminant Analysis (LDA) and Support Vector Machines

(SVM).These techniques have performed well in controlled ecosystem but when the illumination or the lighting effect, body posture and different facial expressions and due to that the accuracy of the recognition got declined.

When compared to more traditional techniques like PCA and LDA the model significantly increases the recognition accuracy [21]. Better feature extraction and capacity against changes in body posture and facial expressions are offered by deep learning algorithms.

However, the first FaceNet architecture which requires a significant amount of processing power and also ignores the genuine problems like the spoofing attacks, automated attendance and other environmental issue s like the low lighting [15].

Usually for practically implementing in the attendance system more modules are required so that we can come up with an advanced and secure model.

2.3 ***Attendance systems using liveness detection***

Blink detection, head movement and facial motion tracking are some of the examples for liveness detection methods which helps us in authenticating the user from spoofing attempts or using a static and printed photos [42]. By rejecting the unauthorized user for the marking of the attendance these methods had significantly increased the system security.

However, several existing methods only focus on anti-spoofing mechanism and doesn't include the IoT connection, picture analysis or automated attendance. Their value in actual attendance system is still ignored.

2.4 ***IoT-Based Automated Attendance Systems***

The use of Internet of Things (IoT) for the attendance management system has been studied by a number of researchers. The real time wireless network communication between the device and the database was demonstrated using an IoT enabled attendance system using an ESP8266 module [50]. Such system primarily improves automatic data synchronization and remote monitoring.

However, a lot of modern IoT based attendance system still uses RFID cards or fingerprint scanners which can be exploited and may need a physical touch too.

Furthermore, most of this system also lacks in advanced facial recognition and liveness verification techniques too.

2.5 ***Low-light face recognition using image enhancement techniques***

To improve the accuracy in facial recognition under low lighting conditions the researchers had conducted a study into a variety of image for improving the methods. A successful way for improving the local contrast while eliminating noise amplification in by implementing the Contrast Limited Adaptive Histogram Equalization (CLAHE) [45].

Based on experimental analysis CLAHE has significantly improved the facial visibility under low lighting conditions and also it improved the recognition accuracy. Despite these advantages the majority of the current projects only focuses on improving the images they don't include the security features like automatic attendance management and liveness detection too.

Table 2.

3. Proposed System Architecture

In this system we have implemented both the software and hardware components that work together for real-time face recognition and verification. The suggested attendance system combines computer vision, deep learning and Internet of Things (IoT) technologies which enables secure and automated attendance monitoring process.

The system has several relevant modules that handle image acquisition, optimization, face recognition, liveness detection and attendance management.

3.1 ***Hardware and Software Requirements***

Table 3.

3.2 ***Image Acquisition Module***

The image acquisition module captures real-time video frames using a webcam that is a part of the system. To improve efficiency and reduce unnecessary processing a PIR motion sensor is connected to the ESP8266 module which continuously monitors for human movement. When motion is detected the ESP8266 automatically starts the face recognition process. This system reduces computational load and power use while allowing for real-time operation.

3.3 ***Pre-processing & Low light enhancement***

To improve image quality and recognition accuracy, the collected image frames undergo pre-processing before going for recognition. Sometimes the facial details may become blurry in low light which reduces the system performance. To address this issue the Contrast Limited Adaptive Histogram Equalization (CLAHE) is used to improve image contrast and brightness adaptively[48]. The developed frames boost facial feature visibility and increase recognition performance under different lighting conditions.

Figure 1.

3.4 ***Face detection and recognition module***

3.4.1. Face detection using dlib

The proposed system uses dlib frontal face detector for real time face detection. The detector detects the human face regions from the live video frames obtained through webcam. Histogram of Orientated Gradients (HOG) based facial detection is used which efficiently and accurately localizes the face with low computational complexity.

The detected facial regions are processed further before recognition to improve the performance and accuracy of the system.

3.4.2 Image preprocessing using CLAHE

Histogram Equalization (CLAHE) is used to improve recognition performance under poor illumination. CLAHE improves local contrast and visibility in low-light conditions without significantly increasing noise.

The preprocessing step results in a significant improvement in the recognition accuracy under low illumination conditions and also enables reliable operation in real world scenarios such as classrooms, offices and corridors [48]. Here the facial noises are reduced to increase the facial enhancements and it also helps in capturing and training of the system.

The histogram equalization function is expressed as:

$$s_k = (L-1)\sum_{j=0}^{k} p(r_j)$$

Where:

s_k= output pixel intensity

L= total number of gray levels

$p(r_j)$= probability distribution of input intensity

r_j= input gray level

The probability distribution is calculated as:

$$p(r_j) = \frac{n_j}{n}$$

Where:

n_j= number of pixels with intensity r_j

n= total number of pixels

CLAHE divides the image into smaller regions called tiles and applies local histogram equalization to improve illumination in an adaptive and efficient way.

3.4.3 ArcFace-based feature extraction

The detected facial image, after preprocessing, is resized to 112×112 pixels and fed into the ArcFace deep learning model for feature extraction. ArcFace produces highly discriminative facial embeddings that uniquely represent facial characteristics in numerical vector format. These embeddings are then compared with stored embeddings using similarity measurement techniques for identity verification[1], [39].

The embedding vector is represented as:

$$F = [f_1, f_2, f_3, \dots, f_n]$$

Where:

F= facial embedding vector

f_i= extracted facial feature values

n= embedding dimension

3.4.4 Tensor Flow and deep learning integration

The facial embeddings generated are saved in the database in the form of floating-point decimal. Each embedding is composed of a number of numerical feature values that depict the specific facial features of the user[39], [41]. The images are stored in a numerical vector value and for that it increases the security of the system and anyone if gets the files or documents he/she can't decrypt the images.

During identification, the new generated embeddings are compared against the stored database embeddings with similarity distance calculation like Euclidean distance or cosine similarity for accurate user identification.

3.4.5 Embedding storage in database

The facial embeddings generated are saved in the database in the form of floating-point decimal. Each embedding is composed of a number of numerical feature values that depict the specific facial features of the user. Hence it increases the security of the system and if anyone gets the files or documents he/she can't decrypt the images.

During identification the new generated embeddings are compared against the stored database embeddings with similarity distance calculation like Euclidean distance or cosine similarity for accurate user identification.

Euclidean Distance for Face Matching:

$$D = \sqrt{\sum_{i=1}^{n} (x_i - y_i)^2}$$

Where:

D= Euclidean distance

x_i= stored face embedding

y_i= input face embedding

n= embedding size

If the calculated distance is below a predefined threshold, the face is recognized as a valid user.

Cosine Similarity for Feature Matching:

$$Similarity(A, B) = \frac{A \cdot B}{|| A ||\times|| B ||}$$

Where:

A= stored face embedding

B= detected face embedding

$A \cdot B$= dot product

$|| A ||$and $|| B ||$= vector magnitudes

3.5 Liveness detection and anti-spoofing

3.5.1 Liveness detection using Eye Aspect Ratio (EAR)

The suggested method helps us in differentiating a real user and spoofing attempts by using a blink-based liveness detection technique [40]. During the verification and authentication process it tracks the eye movement and the blinking patterns through facial landmark analysis. If the system does not detect natural blinking activity the it rejects the authentication process and automatically the user's data gets stored in the system for future analysis.

The Eye Aspect Ratio is calculated as:

$$EAR = \frac{\| p_2 - p_6 \| + \| p_3 - p_5 \|}{2 \| p_1 - p_4 \|}$$

Where:

$p_1, p_2, \ldots, p_6$are eye landmark points.

$\|\cdot\|$ represents Euclidean distance.

Figure 2.

When the Eye Aspect Ratio value falls below the threshold value a blink is detected.

3.5.2 Head movement verification

An unpredictable head movement challenge i.e., left and right movement is ordered during the authentication process. The user must have to perform the necessary movements so that to get authenticated during the liveness

detection stage. This effective challenge & response system improves the security and prevents unauthorized access by using printed photos or static images.

Figure 3.

3.5.3 Blur detection using Laplacian Variance

Therefore, in order to confirm the image clarity for the recognition purpose, here the system additionally performs a blur analysis of the detected image by using the Laplacian variance method [47],[49].

Furthermore, to prevent false detection and increase in accuracy the system automatically rejects low quality image or blurry faces. This mechanism makes the system more reliable in real time and also the detection mechanism gets strengthened by this method.

To detect blurry facial images:

$$Var(L) = \frac{1}{N}\sum_{i=1}^{N}(L_i - \mu)^2$$

Where:

$Var(L)$= variance of Laplacian s

L_i= Laplacian pixel value

μ= mean Laplacian value

N= total number of pixels

If the variance value is below the threshold value of the image than in that case it is considered as blurry and automatically it gets rejected by the system.

3.5.4 Anti-spoofing validation

To detect the fake and false facial inputs an anti-spoofing technique has been implemented in this system so that an unidentified user cannot bypass the system. The anti-spoofing method generally locates the low texture in the facial regions by using a texture analysis and image sharpness method.

These security precautions help to improve the authentication and validation process and make the system more reliable so that it can reduce the possibility of spoofing attacks.

Figure 4: (a) & (b)

3.6 Attendance management module

3.6.1 Automated attendance recording

After the successful face recognition or registration then liveliness detection attendance gets automatically recorded in the database with specific date and time.

The automated attendance system eliminates the manual attendance which reduces the human error in the system.

3.6.2 Duplicate attendance prevention

The anti-spam mechanism in the system prevents the duplicate entries or the attendance in the system. Once the face is recognized or the attendance is marked for the present day then the additional recognition attempts is exempted or ignored for the same user for the same day.

The system automatically shows a pop up or a notification that "**Attendance already marked for the day**" and also it doesn't create any additional database records.

These features improve the overall consistency of the database and also prevents the manipulation of the database and records too.

Figure 5.

3.6.3 Database management

In this system the attendance records & facial embeddings are stored securely for future analysis and retrieval of data in a secured way.

The database module supports attendance history generation as well as exporting the CSV file for further analysis in a detailed manner.

3.7 Unknown face monitoring

3.7.1 Unknown face detection

In this system if the recognition module fails to compare and recognize the detected face stored in the database as an embedding then the user or the face is classified as an **unknown user**.

The unknown face detection feature helps in improving the security monitoring in the restricted situations.

3.7.2 Unknown face storage

The unknown faces get stored separately in another directory so that we can easily monitor, analyze and take certain decisions according to the situation.

This feature helps us in identifying the unauthorized access attempts for different users.

Figure 6.

3.7.3 **IoT-based alert generation**

The ESP8266 module linked with this attendance system help to get the real time alerts during known and unknown face detection events. The buzzers connected with this module provides a real time alerts during the unknown face or unauthorized face detection of any user [11],[24].

Figure 7.

This mechanism improves real-time monitoring and serves overall system security.

4. System Workflow

Figure 8.

5. Performance metrices and mathematical models

5.1 Recognition Accuracy

Recognition accuracy is calculated as:

$$Accuracy = \frac{TP + TN}{TP + TN + FP + FN} \times 100$$

Where:

TP= True Positive

TN= True Negative

FP= False Positive

FN= False Negative

Figure 9.

5.2 Precision

Precision measures the correctness of positive predictions.

$$Precision = \frac{TP}{TP + FP}$$

5.3 Recall

Recall measures the ability of the system to correctly identify valid users.

$$Recall = \frac{TP}{TP + FN}$$

5.4 F1-Score

The F1-score combines precision and recall into a single metric.

$$F1 = 2 \times \frac{Precision \times Recall}{Precision + Recall}$$

5.5 Recognition Rate

The recognition rate of the proposed system is calculated as:

$$Recognition\ Rate = \frac{Correctly\ Recognized\ Faces}{Total\ Faces} \times 100$$

5.6 False Acceptance Rate (FAR)

FAR measures the probability of unauthorized access.

$$FAR = \frac{False\ Acceptances}{Total\ Unauthorized\ Attempts}$$

5.7 False Rejection Rate (FRR)

FRR measures the probability of rejecting authorized users.

$$FRR = \frac{False\ Rejections}{Total\ Authorized\ Attempts}$$

5.8 **Processing Time**

The average recognition processing time is calculated as:

$$T_{avg} = \frac{\sum_{i=1}^{n} T_i}{n}$$

Where:

T_i= recognition time for each frame

n= total number of processed frames

5.9Motion Detection Trigger Logic

The PIR-based IoT activation logic can be represented as:

$$R = \begin{cases} 1, & \text{if motion detected} \\ 0, & \text{otherwise} \end{cases}$$

Where:

$R = 1$activates the recognition system

$R = 0$keeps the system idle

This process reduces the unnecessary processing and improves energy efficiency of the system.

6. Experimental results and Performance analysis

The experimental result show different situations whether the person is known or unknown or the user is in low light or not and also it shows the timestamp at what time the user has registered or authenticated by taking the direct data from the database.

6.1 CLAHE comparison graph

Figure 10: (a) & (b)

6.2 Bar graphs comparison

Figure 11: (a) & (b)

6.3 Line graphs

Figure 12: (a) & (b)

Table 4.

7. Advantages of the proposed system

The suggested attendance system offers several benefits compared to traditional methods of managing attendance. It combines motion detection, face recognition, liveness detection and Internet of Things (IoT) automation to boost both security and efficiency. The system works well even in low lighting conditions whereas other existing system often struggle to do better. Especially due to the use of CLAHE based image processing techniques the system works well in low light too.

The suggested system can avoid spoofing attempts that typically use printed photos or static mobile images for by passing the system and for that we have implemented the liveness detection methods like blink detection and head movement. Additionally, by only triggering the recognition process when any motion is detected the PIR sensor and ESP8266 module has reduced the unnecessary computations. This increases the real-time performance and energy efficiency.

Additional components of the system that includes the automatic attendance, stoppage of duplicate entries i.e., reducing the human biasness and the capturing & monitoring of the unknown faces for future analysis. Because of this it

can be used in business organizations, schools and other secure places. The suggested system can function efficiently in real world situations with improved accuracy and reliability and it is easily scalable which is also cost effective in nature.

Table 5.

8. Limitations of the system

The suggested method works well however there are still some limitations in which we have to work more. The extreme lighting differences, massive facial obstructions or incorrect camera angles can also reduce the recognition accuracy. The liveliness detection and facial recognition process might get affected by rapid head movements and high motion blur.

The current setup mainly allows one face to get verified at a time, which may reduce the efficiency during peak hours. The system also depends on the host's computer's hardware and webcam quality.

For accurate recognition the suggested approach also needs an appropriate dataset registration. The recognition processes may occasionally get affected by certain changes that are brought by facial masks, body posture adjustments or from ageing. Furthermore, for the IoT module to work efficiently there must be a uniform connection between the ESP8266 device and the main system.

9. Future Scope

Deep learning and cloud technologies can be implemented so that we can improve the system. Here large-scale attendance tracking and the application of multi face recognition at a time can be implemented so that it can handle the large crowded areas that are likely possible in future advancement of the project.

Additionally, we can implement cloud database integration for the remote access and centralized attendance management in a single server through the API integration.

System security can be improved by implementing the improved and new anti-spoofing methods such as depth sensing, infrared imaging and 3D face analysis. Mask specific recognition, voice assisted authentication and edge-AI-based optimization for low power device deployment are possible in the upcoming future versions.

In the real-world smart security applications, the use of modern AI accelerates and the advanced of neural network configurations can boost the recognition accuracy, processing speed and the scalability of the software.

10. Conclusion

In this paper, a robust IoT-based facial recognition attendance system included with adaptive low-light advancement and liveness detection techniques. The suggested system offers a secure, automated and real-time attendance management technique by combining the computer vision, deep learning and IoT technologies.

While liveness verification methods like blink detection and head movement analysis provides defense against the spoofing attempts and the application of CLAHE has greatly enhanced the recognition performance in low light environments.

By implementing the ESP8266 module and PIR motion sensor in the system has intelligently activated the recognition process and thus it reduces the unnecessary processing or the computation and also it increases the efficiency of the system.

Therefore, the suggested-approach delivers reliable recognition accuracy with improved security in practical situations which we got during the experimental analysis of the system. While preserving the effective database storage and monitoring capabilities the attendance management module efficiently avoids the duplicate entries during the authentication and verification process thus it removes the human biasness in the system.

For automated attendance tracking in offices, educational institutions and a safe access control conditions the system provides a practical, scalable and affordable solution.

References

[1]T. Schroff, D. Kalenichenko, and J. Philbin, "FaceNet: A unified embedding for face recognition and clustering," in Proc. IEEE Conf. Comput. Vis. Pattern Recognit. (CVPR), 2015, pp. 815–823.

[2] "Face Recognition with OpenCV," OpenCV Documentation, 2025. [Online]. Available: https://docs.opencv.org/4.x/da/d60/tutorial_face_main.html [Accessed: Dec. 9, 2025].

[3] "Face recognition using OpenCV and Python: A beginner's guide," SuperDataScience. [Online]. Available: https://www.superdatascience.com/blogs/opencv-face-recognition [Accessed: Dec. 9, 2025].

[4] "OpenCV Face Recognition," PyImageSearch. [Online]. Available: https://pyimagesearch.com/2018/09/24/opencv-face-recognition/, [Accessed: Dec. 9, 2025].

[5] "FaceNet – Using Facial Recognition System," GeeksforGeeks, 2020. [Online]. Available: https://www.geeksforgeeks.org/machine-learning/facenet-using-facial-recognition-system, [Accessed: Dec. 9, 2025].

[6] "DeepFace," Wikipedia, 2015. [Online]. Available: https://en.wikipedia.org/wiki/DeepFace. [Accessed: Dec. 9, 2025].

[7] S. Sawhney et al., "Real-Time Smart Attendance System using Face Recognition," in Proc. Int. Conf., 2019.

[8] "Face Recognition Based Student Attendance System," IEEE Xplore, 2022.

[9] "Vision-Face Recognition Attendance Monitoring System," IEEE Xplore, 2019.

[10] "Face Recognition Smart Attendance System using Deep Transfer Learning," Procedia Computer Science, vol. 186, pp. 258–265, 2021.

[11] "Automated Facial Recognition Attendance System Leveraging IoT," IEEE Xplore, 2019.

[12] "Face Detection with Python Using OpenCV Tutorial," DataCamp, 2024. [Online]. Available: https://www.datacamp.com/tutorial/face-detection-python-opencv, [Accessed: Dec. 9, 2025].

[13] "Face Recognition Using OpenCV & Python | UNKNOWN Face Recognition," YouTube – Knowledge Doctor, 2023. [Online], Available: https://www.youtube.com/watch?v=LKPB8YM8awk.[Accessed: Dec. 9, 2025].

[14] D. Silver et al., "Mastering the game of Go without human knowledge," Nature, vol. 550, no. 7676, pp. 354–359, 2017.

[15] V. S. Manjula and L. D. S. S. Baboo, "Face detection identification and tracking by PRDIT algorithm using image database for crime investigation," Int. J. Comput. Appl., vol. 38, no. 10, pp. 40–46, Jan. 2012.

[16] K. Lander, V. Bruce, and M. Bindemann, "Use-inspired basic research on individual differences in face identification: Implications for criminal investigation and security," Cognitive Research: Principles and Implications, vol. 3, no. 1, pp. 1–13, Dec. 2018.

[17] Y. Hu, H. An, Y. Guo, C. Zhang, T. Zhang, and L. Ye, "The development status and prospects on the face recognition," in Proc. 4th Int. Conf. Bioinformatics and Biomedical Engineering, Jun. 2010, pp. 1–4.

[18] R. Gottumukkal and V. K. Asari, "An improved face recognition technique based on modular PCA approach," Pattern Recognition Letters, vol. 25, no. 4, pp. 429–436, Mar. 2004.

[19] D. C. Hoyle and M. Rattray, "PCA learning for sparse high-dimensional data," Europhysics Letters, vol. 62, no. 1, pp. 117–123, Apr. 2003.

[20] K. Vijay and K. Selvakumar, "Brain fMRI clustering using interaction K-means algorithm with PCA," in Proc. Int. Conf. Communication and Signal Processing (ICCSP), Apr. 2015, pp. 909–913.

[21] J. Li, B. Zhao, H. Zhang, and J. Jiao, "Face recognition system using SVM classifier and feature extraction by PCA and LDA combination," in Proc. Int. Conf. Computational Intelligence and Software Engineering, Dec. 2009, pp. 1–4.

[22] F. Vogt, B. Mizaikoff, and M. Tacke, “Numerical methods for accelerating the PCA of large data sets applied to hyperspectral imaging,” Proc. SPIE, vol. 4576, pp. 215–226, Feb. 2002.

[23] C. Ordonez, N. Mohanam, and C. Garcia-Alvarado, “PCA for large data sets with parallel data summarization,” Distributed and Parallel Databases, vol. 32, no. 3, pp. 377–403, Sep. 2014.

[24] S. Chintalapati and M. V. Raghunadh, “Automated attendance management system based on face recognition algorithms,” in Proc. IEEE Int. Conf. Computational Intelligence and Computing Research, Dec. 2013, pp. 1–5.

[25] J. Lu, K. N. Plataniotis, and A. N. Venetsanopoulos, “Face recognition using LDA-based algorithms,” IEEE Trans. Neural Networks, vol. 14, no. 1, pp. 195–200, Jan. 2003.

[26] C. Cortes and V. Vapnik, “Support-vector networks,” Machine Learning, vol. 20, no. 3, pp. 273–297, 1995.

[27] A. Sun, E.-P. Lim, and Y. Liu, “On strategies for imbalanced text classification using SVM: A comparative study,” Decision Support Systems, vol. 48, no. 1, pp. 191–201, Dec. 2009.

[28] Y. Freund, R. Iyer, E. R. Schapire, Y. Singer, and T. G. Dietterich, “An efficient boosting algorithm for combining preferences,” J. Mach. Learn. Res., vol. 4, no. 6, pp. 170–178, 2004.

[29] G. Rätsch, T. Onoda, and K.-R. Müller, “Soft margins for AdaBoost,” Machine Learning, vol. 42, no. 3, pp. 287–320, 2001.

[30] Y. Cao, Q.-G. Miao, J. C. Liu, and L. Gao, “Advance and prospects of AdaBoost algorithm,” Acta Automatica Sinica, vol. 39, no. 6, pp. 745–758, Mar. 2014.

[31] Q. W. Wang, Z. L. Ying, and L. W. Huang, “Face recognition algorithm based on Haar-like features and gentle AdaBoost feature selection via sparse representation,” Applied Mechanics and Materials, vol. 742, pp. 299–302, Mar. 2015.

[32] L. I. Xiang-Feng et al., “Vehicle detection algorithm based on improved AdaBoost and Haar,” Measurement & Control Technology, Feb. 2019.

[33] J. Deng, J. Guo, N. Xue, and S. Zafeiriou, “ArcFace: Additive Angular Margin Loss for Deep Face Recognition,” in Proc. IEEE/CVF Conf. Computer Vision and Pattern Recognition (CVPR), 2019, pp. 4690–4699.

[34] F. Schroff, D. Kalenichenko, and J. Philbin, “FaceNet: A Unified Embedding for Face Recognition and Clustering,” in Proc. IEEE CVPR, 2015, pp. 815–823.

[35] O. M. Parkhi, A. Vedaldi, and A. Zisserman, “Deep Face Recognition,” British Machine Vision Conference (BMVC), 2015.

[36] Y. Taigman, M. Yang, M. Ranzato, and L. Wolf, “DeepFace: Closing the Gap to Human-Level Performance in Face Verification,” Proc. IEEE CVPR, 2014, pp. 1701–1708.

[37] Q. Cao, L. Shen, W. Xie, O. M. Parkhi, and A. Zisserman, “VGGFace2: A Dataset for Recognising Faces Across Pose and Age,” IEEE FG, 2018.

[38] A. Georghiades, P. Belhumeur, and D. Kriegman, “From Few to Many: Illumination Cone Models for Face Recognition Under Variable Lighting and Pose,” IEEE TPAMI, vol. 23, no. 6, pp. 643–660, 2001.

[39] K. He, X. Zhang, S. Ren, and J. Sun, “Deep Residual Learning for Image Recognition,” IEEE CVPR, 2016.

[40] A. Krizhevsky, I. Sutskever, and G. Hinton, “ImageNet Classification with Deep Convolutional Neural Networks,” NIPS, 2012.

[41] K. Zhang, Z. Zhang, Z. Li, and Y. Qiao, “Joint Face Detection and Alignment Using Multi-task Cascaded Convolutional Networks,” IEEE Signal Processing Letters, 2016.

[42] G. Pan, L. Sun, Z. Wu, and S. Lao, “Eyeblink-based Anti-Spoofing in Face Recognition,” Int. Conf. Biometrics, 2007.

[43] Z. Boulkenafet, J. Komulainen, and A. Hadid, "Face Anti-Spoofing Based on Color Texture Analysis," IEEE ICIP, 2015.

[44] A. George and S. Marcel, "Deep Pixel-wise Binary Supervision for Face Presentation Attack Detection," ICB, 2019.

[45] K. Zuiderveld, "Contrast Limited Adaptive Histogram Equalization," Graphics Gems IV, Academic Press, 1994, pp. 474–485.

[46] R. C. Gonzalez and R. E. Woods, "Digital Image Processing," 4th Edition, Pearson, 2018.

[47] N. Dalal and B. Triggs, "Histograms of Oriented Gradients for Human Detection," IEEE CVPR, 2005.

[48] ESP8266 Technical Reference Manual, Espressif Systems, 2024.

[49] PIR Motion Sensor User Guide, HC-SR501 Technical Documentation, 2024.

[50] A. Kumar and K. Singh, "IoT-Based Smart Attendance System Using Face Recognition," International Journal of Advanced Computer Science and Applications, vol. 12, no. 4, pp. 210–217, 2021.

Figure's captions:

Figure 1: The effect of CLAHE Analysis taken from the facial images in low light environments. When compared with the original images the enhanced images perform well and also displays better with brightness, contrast and facial features. This preprocessing step improves recognition accuracy in low light conditions.

Figure 2: Eye Aspect Ratio (EAR) used for blink detection or liveness detection in the suggested system which uses six facial landmarks around the. The EAR value decreases when the eye is closed and also it remains constant with the eyes are open.

Figure 3: Head movement mechanism used forliveness detection and the user have to perform certain challenges that are system generated and also this mechanism helps to stop the spoofing attacks.

Figure 4:(a) and (b) Anti Spoof Validation helps to detect the fake detected images as it compares with the data stored in the database in the form of facial embeddings.

Figure 5: Attendance Prevention Mechanism helps to stop the duplicate entries on a user as one user cannot do multiple entries in the system and once the face is recognized the database automatically record the data.

Figure 6: Unknown faces stored in the database whenever the system fails to detect the individual it automatically sores the data in a separate directory and assists the admin for future analysis.

Figure 7: Active buzzer which is used for security alerts is integrated with the ESP8266 module so that due to unauthorised access the admin can get a clear and audible alerts from the system and also improves the real time monitoring system.

Figure 8: Fully automated AI with smart automated system which reduces the unnecessary computation through the IoT sensors and improves the efficiency of the system.

Figure 9: Pie graph used for recognition analysis provides a visual representation of the system and also demonstrates the recognition performance under different conditions.

Figure 10:CLAHE analysis of two different lighting conditions which shows significant analysis under different lighting conditions with clear visibility, contrast and are more reliable for the feature extraction procedure.

Figure 11: Analysis for authorised and unauthorised access provides the number of users tried and authenticated during the execution process with comparing the data stored in the database.

Figure 12: :(a) and (b) Line graphs for different counts provides a visual output throughout the operational period with specific timestamps and also shows the data of know and unknown users.

Table's captions:

Table 1: Different generations of the attendance management systems: the suggested approach uses CLAHE implementation and also have liveness detection with IoT technology while the traditional systems have certain limitations like low lights and are also prone to errors.

Table 2: Comparison between the present and existing systems which clearly states that through deep learning technology and also with advanced modules we can make a secure and easily scalable system.

Table 3: Hardware & Software requirements which are required for the suggested system, which is easily affordable and also gives a secure system with all the advanced modules.

Table 4: Performance metrics of the suggested system with high accuracy and low false acceptance and rejection rate also by maintaining the processing time for real time deployment

Table 5: Comparison with the existing face recognition algorithms where the suggested method achieved better recognition accuracy under low light and also through liveness detection and IoT based system.

Figures:

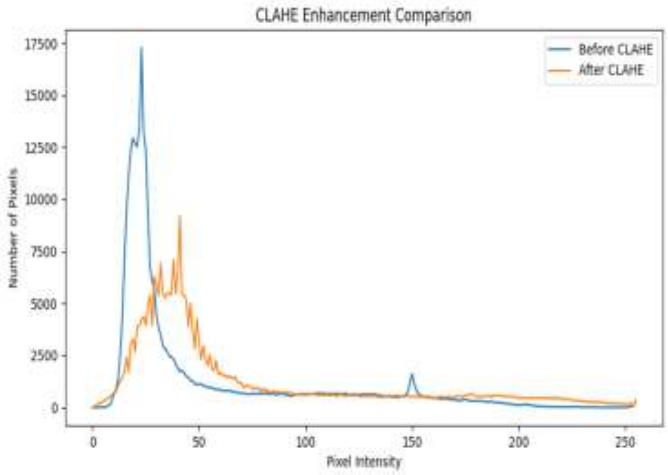


Figure 1: The effect of CLAHE Analysis taken from the facial images in low light environments. When compared with the original images the enhanced images perform well and also displays better with brightness, contrast and facial features. This preprocessing step improves recognition accuracy in low light conditions

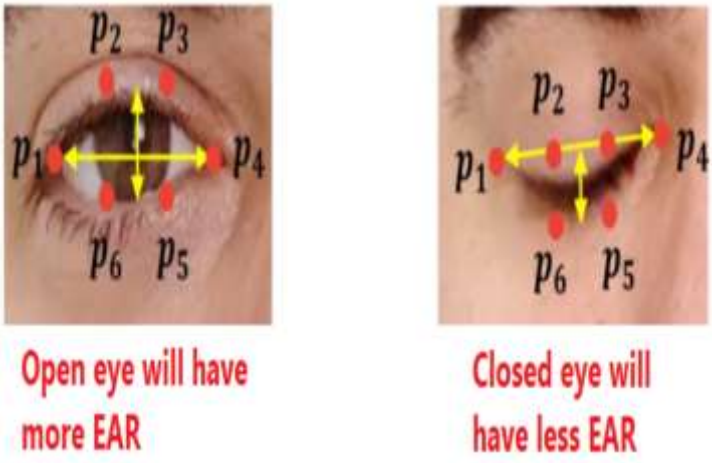


Figure 2: Eye Aspect Ratio (EAR) used for blink detection or liveness detection in the suggested system which uses six facial landmarks around the. The EAR value decreases when the eye is closed and also it remains constant with the eyes are open.

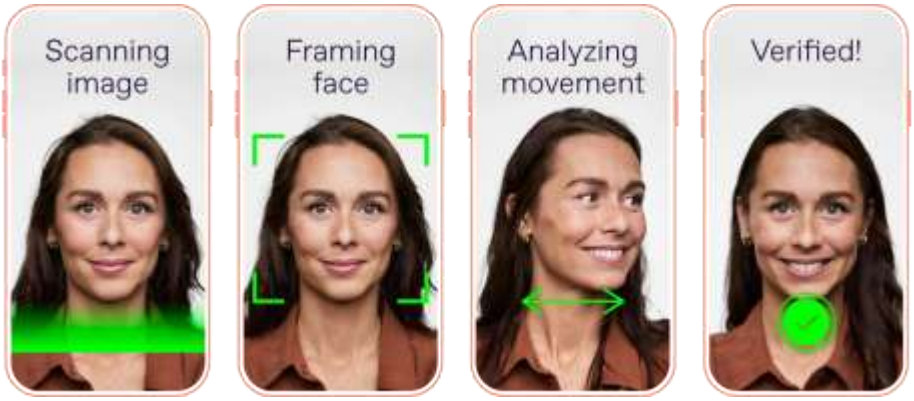


Figure 3: Head movement mechanism used forliveness detection and the user have to perform certain challenges that are system generated and also this mechanism helps to stop the spoofing attacks.



(a)



(b)

Figure 4: (a) and (b) Anti Spoof Validation helps to detect the fake detected images as it compares with the data stored in the database in the form of facial embeddings.

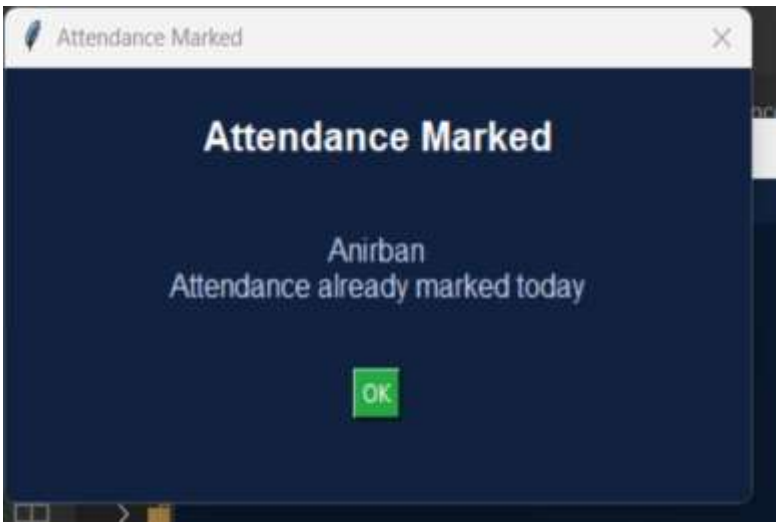


Figure 5: Attendance Prevention Mechanism helps to stop the duplicate entries on a user as one user cannot do multiple entries in the system and once the face is recognized the database automatically record the data.

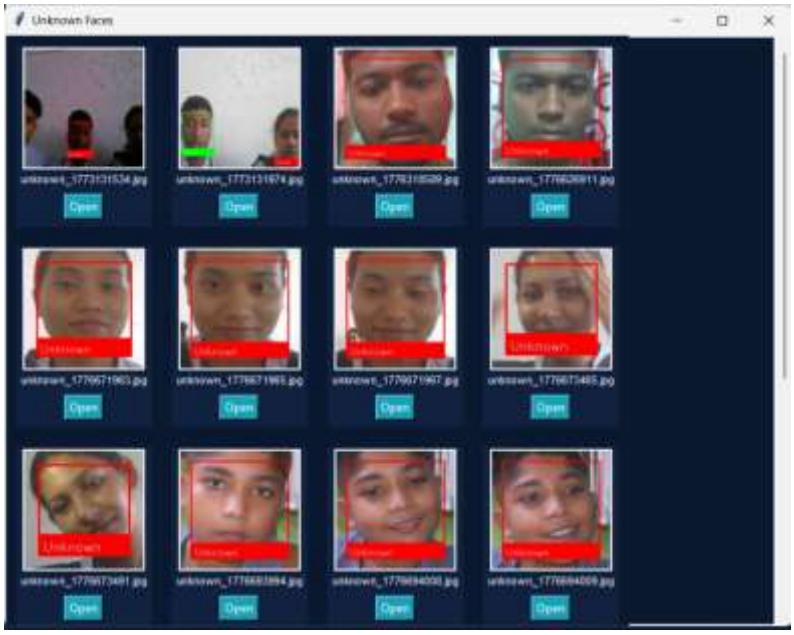


Figure 6: Unknown faces stored in the database whenever the system fails to detect the individual it automatically sores the data in a separate directory and assists the admin for future analysis.



Figure 7: Active buzzer which is used for security alerts is integrated with the ESP8266 module so that due to unauthorised access the admin can get a clear and audible alerts from the system and also improves the real time monitoring system.

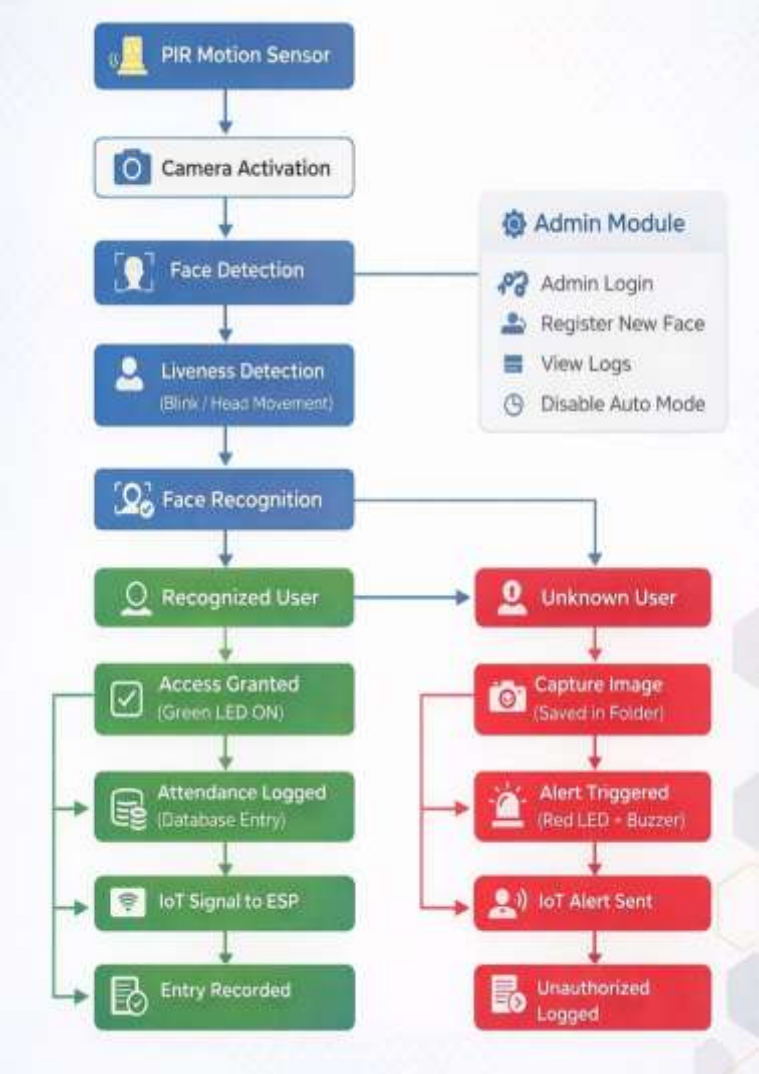


Figure 8: Fully automated AI with smart automated system which reduces the unnecessary computation through the IoT sensors and improves the efficiency of the system.

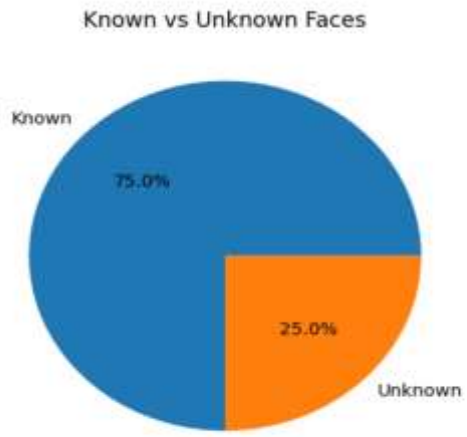
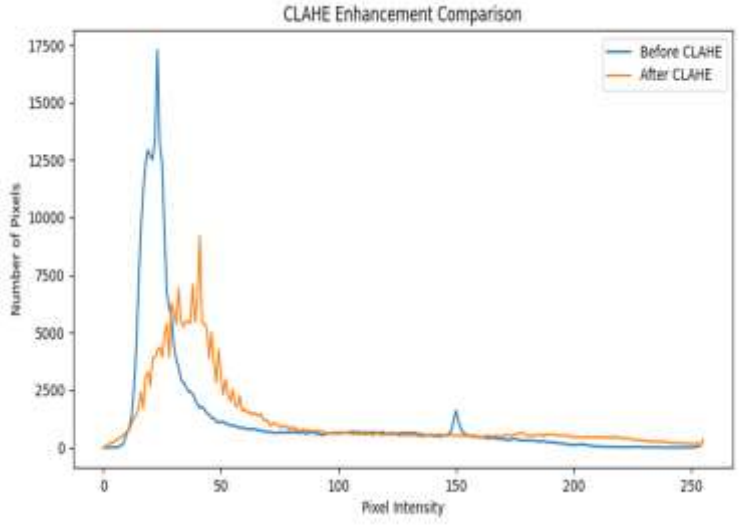
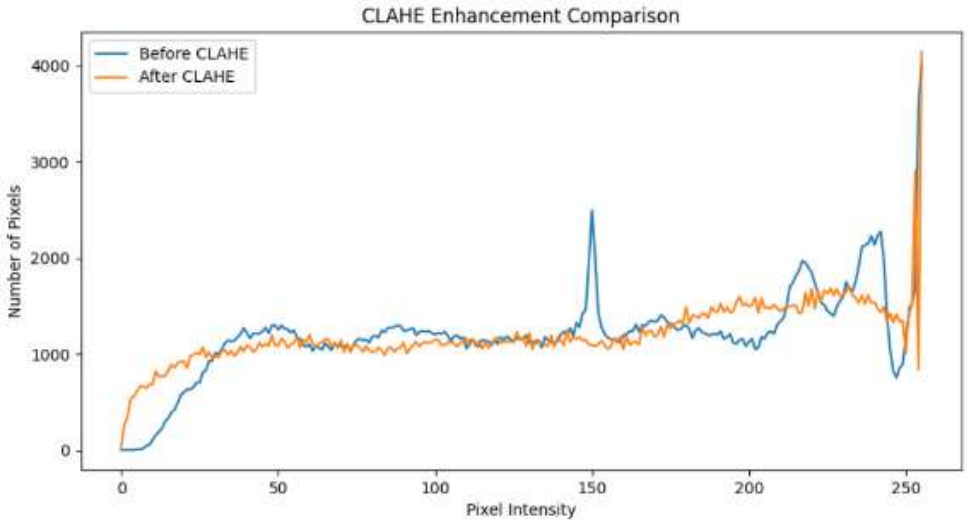


Figure 9: Pie graph used for recognition analysis provides a visual representation of the system and also demonstrates the recognition performance under different conditions.

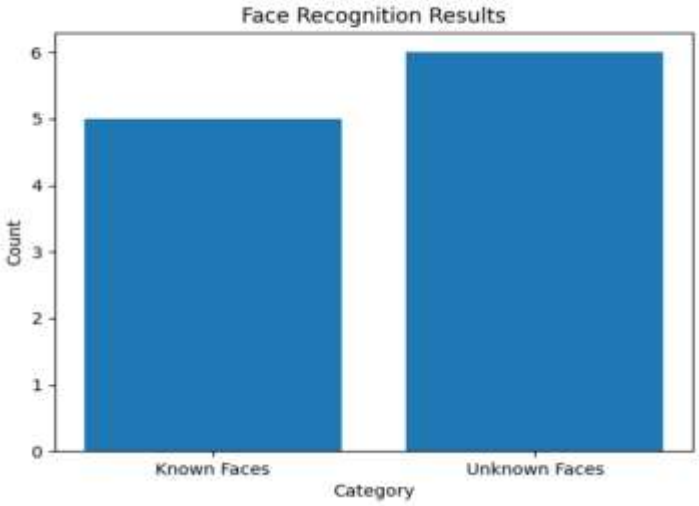


(a)

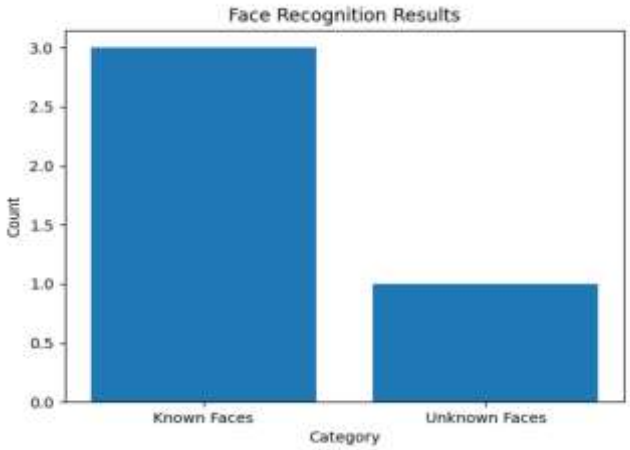


(b)

Figure 10: CLAHE analysis of two different lighting conditions which shows significant analysis under different lighting conditions with clear visibility, contrast and are more reliable for the feature extraction procedure.

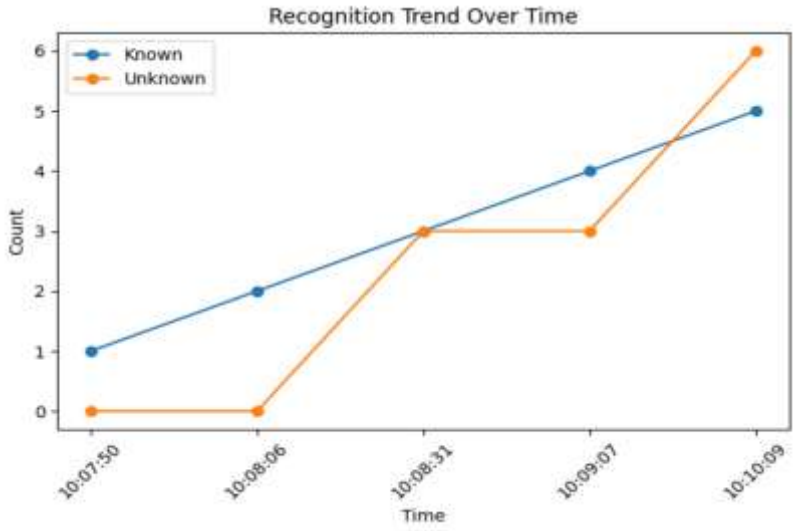


(a)

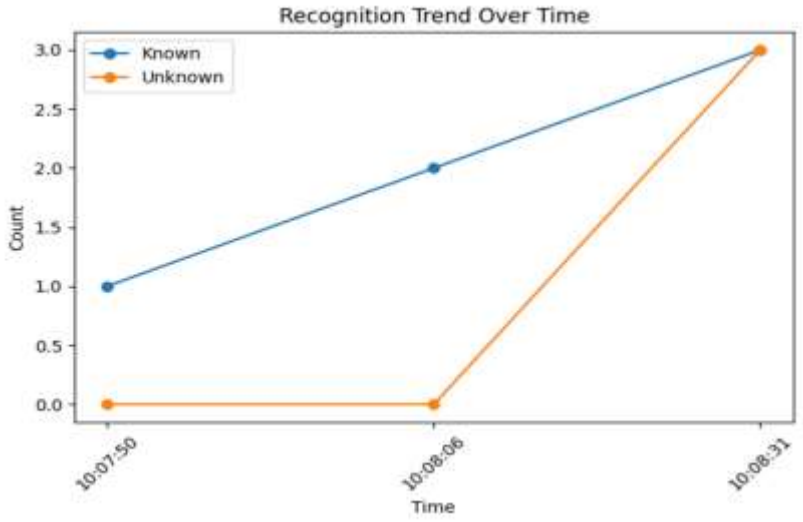


(b)

Figure 11: Analysis for authorised and unauthorised access provides the number of users tried and authenticated during the execution process with comparing the data stored in the database.



(a)



(b)

Figure 12: (a) and (b) Line graphs for different counts provides a visual output throughout the operational period with specific timestamps and also shows the data of know and unknown users.

Tables:

Stage	Technologies	Characteristics
Traditional Attendance	Manual register, RFID	Time-consuming, less secure
Basic Face Recognition	OpenCV, Haar Cascade	Real-time detectionbut weak in low light
Deep Learning Stage	Face Net/Arc Face, TensorFlow	Better recognition accuracy
Proposed Smart IoT System	CLAHE, Liveness Detection, ESP8266, PIR Sensor	Low-light support, anti-spoofing, energy efficient automation

Table 1: Different generations of the attendance management systems: the suggested approach uses CLAHE implementation and also have liveness detection with IoT technology while the traditional systems have certain limitations like low lights and are also prone to errors.

Author	Technique Used	Advantage	Limitation
Chintalapati et al. (2013)	Face Recognition	Automated attendance	No anti-spoofing
Schroff et al. (2015)	FaceNet	High accuracy	High computation
IoT Attendance System (2019)	ESP8266	Remote monitoring	No liveness detection
CLAHE-based Recognition (2022)	CLAHE	Better low-light performance	No attendance automation
Proposed System	Face Recognition + CLAHE + Liveness + IoT	High accuracy, anti-spoofing, automation	Limited to single-camera deployment

Table 2: Comparison between the present and existing systems which clearly states that through deep learning technology and also with advanced modules we can make a secure and easily scalable system.

Component	Description
Webcam	HD USB Camera
ESP8266	IoT Communication Module
PIR Sensor	Motion Detection
Processor	Intel i5
RAM	8 GB
Programming Language	Python
Libraries	Open CV,dlib, Tensor Flow
Database	SQLite/MySQL

Table 3: Hardware & Software requirements which are required for the suggested system, which is easily affordable and also gives a secure system with all the advanced modules.

Parameter	Value
Recognition Accuracy	96.4%
Precision	95.8%
Recall	94.9%
FAR	2.1%
FRR	3.4%
Average Processing Time	0.8 sec

Table 4: Performance metrics of the suggested system with high accuracy and low false acceptance and rejection rate also by maintaining the processing time for real time deployment

Algorithm	Recognition Accuracy (%)	Low-Light Support	Liveness Detection	IoT Integration
PCA (Eigenfaces)	84.2	Poor	No	No
LBPH	88.5	Moderate	No	No
FaceNet	94.3	Good	Partial	No
Proposed ArcFace + CLAHE System	**97.8**	**Excellent**	**Yes**	**Yes (ESP8266 + PIR)**

Table 5: Comparison with the existing face recognition algorithms where the suggested method achieved better recognition accuracy under low light and also through liveness detection and IoT based system.