Attendance Monitoring System Using Facial and Geo-Location Verification

Garima Singh(✉), Monika kumari, Vikas Tripathi, and Manoj Diwakar

Graphic Era (Deemed to Be) University, Dehradun, Uttarakhand, India
garimasinghgryffindor@gmail.com, {vikastripathi.cse, dr.manojdiwakar}@geu.ac.in

Abstract. Face verification is the most distinctive method used in the most effective image processing software, and it is essential in the technical world. Face verification is a method that can be used instead of face recognition. Face recognition is the act of recognising a person from a given image, whereas face verification is the process of confirming that a given face belongs to a particular person. As a result, after the face is validated, the attendance is automatically recorded, and an update is sent. In addition, an anti-spoofing measure of liveness detection is considered to ensure that the system is foolproof. Eye-blink has been used to detect liveness. Additionally, the geographical coordinates of the user are also verified before the attendance is marked. The creation of this system aims to digitalize the outdated method of collecting attendance by calling names and keeping pen-and-paper records. Because current methods of taking attendance are cumbersome and time-consuming.

Keywords: Attendance Monitoring System · Facial Verification · Geo-location Verification

1 Introduction

Attendance management's main aim is to track the working or office hours of employees, faculty as well as students in college. The old method of attendance marking system is a very lengthy task in many schools and colleges. It does create a big work-load on faculty as they have to manually keep a record or documentation of students being present or absent which might take about 5 to 10 min of the entire session. This is time-consuming for students as well as for the faculties too. There are also some chances of proxy attendance. To reduce this many universities and colleges have started deploying many other techniques for recording attendance like Radio Frequency Identification(RFID), iris recognition, face recognition, face recognition with GSM Notification [1].

Biometric-based techniques have emerged as the most promising option for recognizing individuals in recent years since, instead of authenticating people and granting them access to physical and virtual domains based on passwords, PINs, smart cards, plastic cards, tokens, keys and so forth, these methods examine an individual's physiological and/or behavioral characteristics in order to determine and/or ascertain his

B. J. Choi et al. (Eds.): IHCI 2023, LNCS 14531, pp. 406–416, 2024.
https://doi.org/10.1007/978-3-031-53827-8_36

identity. Passwords and PINs are hard to remember and can be stolen or guessed; cards, tokens, keys and the like can be misplaced, forgotten, purloined or duplicated; magnetic cards can become corrupted and unreadable. However, an individual's biological traits cannot be misplaced, forgotten, stolen or forged [2]. Biometric characteristics, such as iris recognition, which are employed for security purposes for limited areas in some organisations, can be utilised to track attendance [3]. The initiative by M. Khari et al. to create a software product that enables facial recognition for admission and leave from metro platform gates. A smart attendance monitoring system can employ a similar strategy [4].

The primary goal of developing an attendance system was to use the verification technique and involve the general public in order to assess its potential benefits for the educational system. Here, the face of a person and their location are taken into account while recording attendance [5]. Since the population is growing by 0.81% year [6], the attendance system is becoming monotonous and wearying. To enable comparisons across organisations and jurisdictions, educational entities are being asked more frequently to report attendance data in a uniform manner. The correlation between student attendance and academic achievement is the main justification for high-quality attendance data [7].

2 Literature Review

According to the research paper [8], the author spoke about how in Covid-19 the biggest problem with inability in normal life was going to in-person classes, attending programs and going to jobs have been impossible without a large amount of risk being involved. In order to make sure educational institutes can function properly and efficiently over an internet connection, they devised a system which was given the title "Attendance management system based on face recognition". The proposed system aims to improve the already existing systems for video conferences that have poor attendance management systems, as also it tries to cover the gap between attendees and hosts by providing features other than just detection of faces and analysis of attendance like keeping track of students. The algorithm used here was converting an RGB image to greyscale and then focusing on one grid of 8 * 8 pixels for each pixel, horizontal and vertical gradients are calculated and then calculated gradient magnitude and gradient angle for each of 64 pixels are compressed and for which histogram of magnitudes and angles are plotted. Now with that 8 * 8 grid will slide along the whole image and after interpreting the full histogram and plotting the HOG features find that the structure of the object or face is well maintained, losing all the insignificant features.

Kowsalya et al. [9] developed a face recognition algorithm-based automatic attendance management system. The camera at the entrance records each person who enters the classroom. After that, the face region is removed and prepared for further processing. Face detection requires less labour because more than one person can be in the entire classroom at once. Face recognition has advantages over other systems that have been discussed for analysing facial recognition and recording attendance. Issues like occlusion persist in this system. There is a high possibility of a person being present and still not being marked present.

Bah et al. [10] study project had two major sections: While the second half concentrated on the attendance management system based on the identified human faces, the first section primarily focused on strengthening the face recognition algorithm. To capture images of employees entering an office or building, a digital live camera will be used in the first section. To improve the quality of the images, advanced image processing techniques, such as contrast adjustment, noise reduction using bilateral filter, and image histogram equalisation, will be applied to the captured images. Next, the Haar Algorithm will be applied to the images to detect specific faces, which will then be used as an input to the Facial Recognition System. The system fails to provide anti-spoofing capabilities.

Some techniques require minimal user involvement and rely exclusively on face recognition. These techniques are also integrated with CCTV systems. When there is a gathering of people in the CCTV feed, this system automatically records attendance [11]. Face Recognition, not Face Verification, is employed in this instance; the two are distinct. Face Verification includes verifying a person's identity by comparing their face with a template that has been stored. It is a one-to-one comparison that is utilised for authentication. In face recognition, a person is recognised by their face being compared to a database of reference pictures. It is a one-to-many comparison that is used to identify someone. Therefore, it is reasonable to say that Face Recognition takes longer because there are more comparisons. Additionally, this technique is not very reliable because there is a chance that some areas may not be covered by the cameras, and occlusion may prevent some people from being marked as present. Systems that rely on facial recognition and verification exist, however, they are easily deceived by spoofing attempts.

The proposed method requires each user to mark their attendance and is not an automatic system like the CCTV-based attendance marking system. The user must log in and engage with the system. Facial Verification would function far better to match the face than Face Recognition, which has a higher Time-Complexity since the user must be logged in before marking the attendance. Additionally, this approach is easily spoofable, necessitating the use of reliable anti-spoofing. It is necessary to use a liveness detection system. Eye-blink has been used to identify liveness. Additionally, we included a function that checks the user's geographic location to ensure that they are indeed at the institution or office. This feature makes our system even more secure.

3 Proposed System

The proposed system improves the existing attendance monitoring system by using Biometric Facial data (i.e.; Inherence factors) (see Fig. 1) for the authentication purpose, which is the highest level of authentication in a 3-Factor Authentication. A 3-factor authentication (3FA) uses three different types of authentication elements to confirm a user's identity. The information or traits that a user must submit as proof of their identity in order to utilise a system, application, or resource are known as authentication factors. In 3-factor authentication, the following three factors are frequently used: Something You Know: This is the standard knowledge-based security measure, such as a password, PIN, or responses to security questions. Only the authorised user should be aware of it, Something You Have: Possession of a tangible item that is specific to the user, such as a smartphone, a security token, or a smart card, constitutes this factor. One-time codes, which the user must supply during the authentication procedure, are generated or received by this object, Something you are: This element uses biometric data, such as voice, facial, or retinal scans, fingerprint, or retinal scans. Biometric information is a reliable authentication component since it is challenging to fake or duplicate.

Here, in our system, we are also using geographical location checks (see Fig. 1) using the coordinates of the user to make the system even more strict and precise. Thereby adding another factor to our 3FA, which makes the system even more secure and difficult to fool. All the steps are shown in Fig. 1. The following steps explain how the proposed system works:

1. While registering the user will provide a photo of his/her face to be saved in the database for matching in the later phase.
2. The user login their account with their ID and Password. This is the first factor of a 3FA which is “what you know”. We can also use OTP here after this step to encompass the second factor of “what you have” as well.
3. Marking the attendance of a particular class will only be enabled in its time slot.
4. Also, the button that will allow the marking of attendance will only be enabled when the geographical coordinates of the user match the geographical coordinates of the Institution (which will be set during the deployment).
5. After the Time Slot check and Geographical Check the button to mark the attendance will be enabled. As and when the user will click on this button, the webcam will be activated.
6. The user will be required to capture their photos. After the spoofing analysis is performed. Then the picture is compared to the original data in the database linked with that account.
7. If matched, the user is required to capture the photo of the faculty whose lecture is being conducted. If the face is matched, the user will be finally verified for attendance and will be marked present in the database. Thereby accomplishing the third factor of the 3FA.

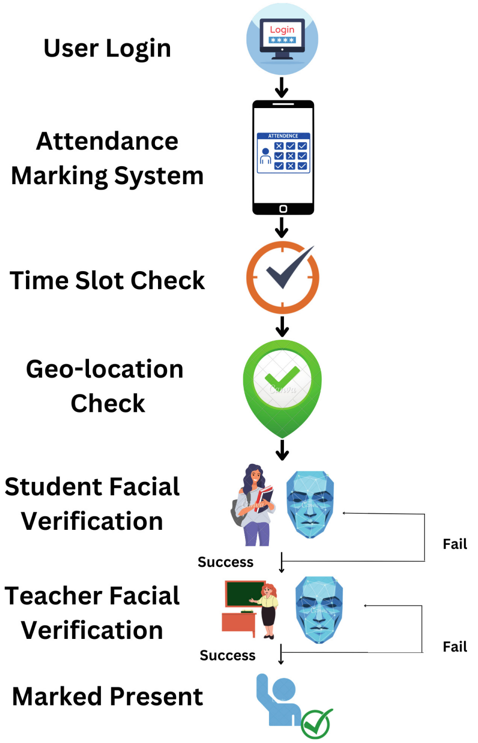


Fig. 1. The overall design of the suggested method to allow attendance marking without any spoofing efforts

3.1 Facial Verification

The facial verification part of the proposed system is divided into the following four phases (see Fig. 3):

Face Detection. A computer vision technology called face detection is used to recognise and locate human faces in digital photos or video frames (see Fig. 3). It is an essential stage in many applications, such as security systems, facial identification, and emotion analysis. The main objective of face detection is to identify any faces in a frame of an image or video and, if any are present, to return the coordinates of the bounding boxes around those faces.

Face Embeddings Extraction. Before we can apply the algorithms that will compare the faces for verification, the face detected in the above step (which is still in the image form) needs to be converted into information or a numerical vector (see Fig. 3) that the algorithm can understand and operate on. The system computes measures based on landmarks and face characteristics like the eyes, nose, and mouth to obtain these embeddings. 68 facial landmarks (see Fig. 2), often called facial keypoints [12].

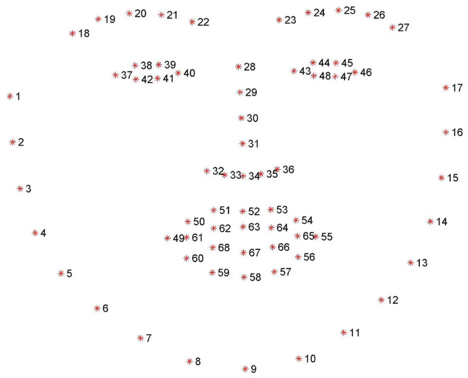


Fig. 2. Sample Facial Landmarks. Picture from PyImageSearch, Adrian Rosebrock [13]

Face Matching. The technique of verifying whether or not two provided face photos belong to the same individual is known as face verification (see Fig. 3). It entails determining whether a person is who they say they are, in other words. Either the faces match (belong to the same person) or they don't, which is typically a binary choice. The more comprehensive problem of face recognition is determining a person's identification from a set of known people. Face recognition, unlike verification, does not involve a binary choice of "same" or "different". Instead, it seeks to narrow down the candidate identities in order to identify the person. For matching faces, we are using verification instead of recognition. Face verification is frequently used for tasks including employing facial recognition to unlock devices, gaining access to protected locations, or verifying people for online transactions [14].

Anti-spoofing. Systems for facial recognition and verification must include anti-spoofing (see Fig. 3) in order to guarantee the process' security and reliability. It is intended to stop attackers from getting around these defences by employing fictitious representations of faces, such as 2D images, films, masks, or other manufactured tools [15]. Anti-spoofing methods try to spot irregularities or discrepancies in the given face that point to a spoofing attempt. These techniques can involve analyzing various factors such as texture, depth, motion, liveness, and even physiological responses like blood flow or blinking (see Fig. 3) [16].

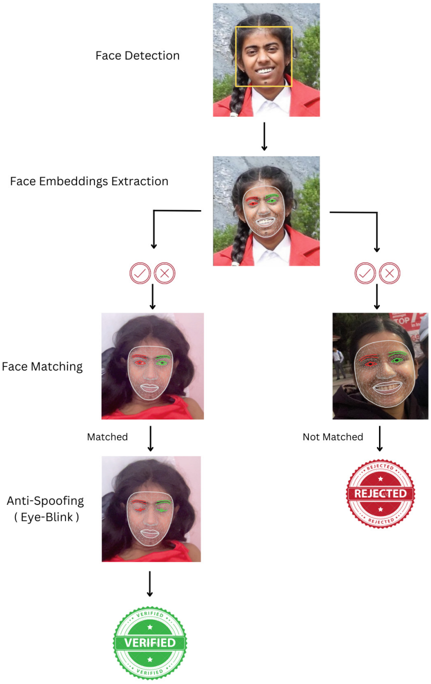


Fig. 3. Step-by-step Facial Verification Process

3.2 Face Detection

We are using MTCNN (Multi-task Cascaded Convolutional Networks) for Face Detection. It is a modern tool to detect faces, consisting of three stages of convolutional networks. The representation of the effective working of all three stages is given in Fig. 4.

Stage 1: P-Network (Proposal-Network). To recognise faces of various sizes, the image is resized numerous times. Here, the threshold for detection is low and hence, many false positives (see Fig. 4) but it is all intentional. It is supposed to work like that. The low detection threshold used by the P-network means that it is sensitive to even subtle face-like features in the image. This sensitivity helps in capturing potential faces that might be missed if a higher threshold were used. While this sensitivity leads to more false positives, it ensures that actual faces are not overlooked [17].

Stage 2: R-Network (Refine-Network). The output from the P-Net is the input to this network. Here, many false positives received from the above network will be rectified (see Fig. 4). And we will obtain precise bounding boxes [17].

Stage 3: O-Network (Output-Network). This is the final stage. Final filtering happens here and also we obtain very precise bounding boxes (see Fig. 4) [17].

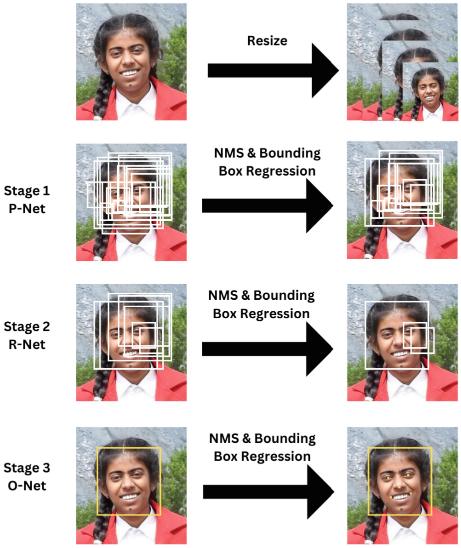


Fig. 4. Face detection with the MTCNN method.

3.3 Facial Embeddings Extraction

For Facial Embeddings extraction, we are using Keras-VGGFace Model. We are using only feature extraction layers of the model with VGGFace(include_top = False) initiation. Keras-VGGFace is a popular deep-learning model implementation in Keras that is specifically designed for face recognition tasks. It is based on the VGG16 architecture, which is a deep convolutional neural network (CNN) model originally developed for image classification.

3.4 Face Matching

The process of detecting whether two face photographs belong to the same person or not is known as facial verification. Therefore, the task effectively consists of calculating the separation between two face vectors or embeddings acquired from the previous stage [18]. Therefore, this step of appropriate distance metrics is critical for facial verification accuracy.

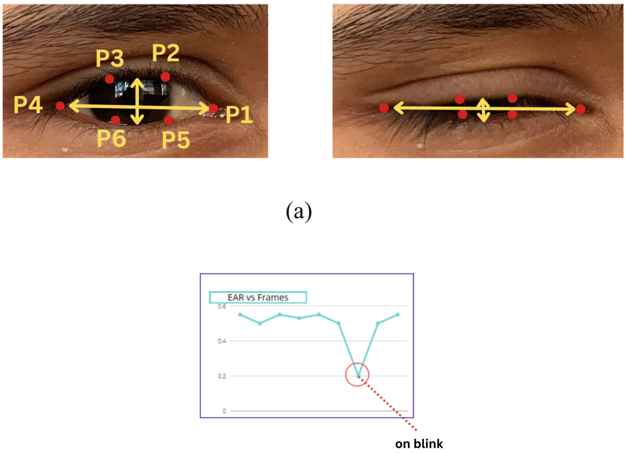
For facial verification, we employ a metric called the cosine similarity. This technique has the best accuracy recorded in the literature when tested on the cutting-edge dataset Labelled Faces in the Wild (LFW) [18].

3.5 Anti-spoofing

Eye-Blink Detection. In order to detect any spoofing attempts we need some form of liveness detection. For that, we are proposing Eye-blinking based liveness detection. For the purpose of detecting eye blinks, OpenCV, Python, and dlib are used. In addition to the imutils package, which contains several functions that will enable us to convert the landmarks to a NumPy array, we are using the dlib library for facial recognition [19]. The following are the main steps for eye-blink detection:

1. Using dlib to detect facial landmarks:
   Using the face landmark detector from the dlib library, one can detect facial landmarks. [19].
2. Eye Landmarks:
   Because we can extract any facial characteristic from the 68 Facial Landmarks discovered in the preceding stage. As a result, we will extract the ocular landmarks, which are 6 (x, y) (see Fig. 5(a)) coordinates for each eye [19].
3. Eye Aspect Ratio (EAR)
   This ratio establishes a link between the horizontal and vertical measures of the eye. [17]. The formula to calculate EAR can be referred from Eq. (1).

$$EAR = \frac{SumofVerticalDistance}{2 * HorizontalDistanceofEye} \tag{1}$$



(a)

(b)

Fig. 5. (a) Opened Eye & Eye when blinked (b) EAR graph when the eye is blinking [19]

When the eye is opened (see Fig. 5(a)), the EAR remains constant, but it abruptly drops (see Fig. 5(b)) when the eye is blinked (see Fig. 5(b)). The average of the EAR from both eyes will be retained. Then, we'll see if it falls below a predetermined threshold (see Fig. 5(b)).

When the EAR falls below the predetermined threshold, we shall keep track of those frames. And if the count matches the predetermined count (as determined by the FPS), it might be 4 or 5, etc. A blink is only regarded as a blink after that.

3.6 Geographic Location Verification

Along with facial verification, the students will also be required to verify their locations. Because of this, the system so build is even stronger, and the system bypassing attempts possibilities would be narrowed. All the conditions to be satisfied in order for the attendance to be marked are illustrastrated in Fig. 6.

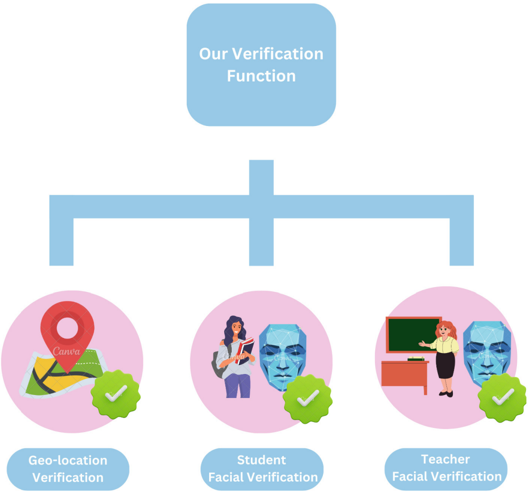

Our Verification Function
Canva
Geo-location Verification
Student Facial Verification
Teacher Facial Verification

Fig. 6. Verification aspects we are considering - (1) Geo-location, (2) Student's Face, and (3) Teacher's Face.

4 Conclusion

From this system, we found out that Attendance Monitoring System is required in every field whether it comes to universities, schools or offices. Face verification will reduce the time of marking attendance. Along with facial verification, we also added functionality to capture the geolocation of the user and verify it as well. Most notably, the system does not rely on a widely used system as in [20] to automatically take pictures of everyone there and mark their attendance; in that scenario, there is a great likelihood that attendance won't be marked owing to problems like occlusion. By requiring user interaction to register their own attendance, our approach lowers the likelihood of fake absences. We added an anti-spoofing mechanism for liveness detection which involves eye-blink detection, but it can also be spoofed. Therefore, the system can be further improved by adding a number of other liveness detection strategies as well like texture analysis, 3D depth analysis, reflection analysis, behavioural analysis etc. Overall an idea has been presented in the paper which although has scope for further improvement but carries the potential to be incorporated as a real-life application.

The author has used her own image to showcase the result and have no issue on publishing her image in the paper.

References

1. Patel, U.A., Priya, S.: Development of a student attendance management system using RFID and face recognition: a review. Int. J. Adv. Res. Comput. Sci. Manage. Stud. **2**(8), 109–119 (2014)
2. Jafri, R., Arabnia, H.R.: A survey of face recognition techniques. J. Inf. Process. Syst. **5**(2), 41–68 (2009)
3. Dua, M., Gupta, R., Khari, M., Crespo, R.G.: Biometric iris recognition using radial basis function neural network. Soft. Comput. **23**(22), 11801–11815 (2019)
4. Dalal, R., Khari, M., Arbab, M.N., Maheshwari, H., Barnwal, A.: Smart metro ticket management by using biometric. In: Multimodal Biometric Systems, pp. 101–110. CRC Press (2021)
5. Puthea, K., Hartanto, R., Hidayat, R.: A review paper on attendance marking system based on face recognition. In: 2017 2nd International Conferences on Information Technology, Information Systems and Electrical Engineering (ICITISEE), pp. 304–309. IEEE (2017)
6. macrotrends. https://www.macrotrends.net/countries/IND/india/population-growth-rate
7. Aden, A.A., Yahye, Z.A., Dahir, A.M.: The effect of student's attendance on academic performance: a case study at Simad university Mogadishu. Acad. Res. Int. **4**(6), 409 (2013)
8. Nalini, N.: Attendance monitoring system based on face recognition (2021)
9. Kowsalya, P., Pavithra, J., Sowmiya, G., Shankar, C.K.: Attendance monitoring system using face detection & face recognition. Int. Res. J. Eng. Technol. (IRJET) **6**(03), 6629–6632 (2019)
10. Bah, S.M., Ming, F.: An improved face recognition algorithm and its application in attendance management system. Array **5**, 100014 (2020)
11. Rakshitha, S.: Face based CCTV attendance monitoring system using deep face recognition (2021)
12. Hangaragi, S., Singh, T., Neelima, N.: Face detection and recognition using face mesh and deep neural network. Procedia Comput. Sci. **218**, 741–749 (2023)
13. pyimagesearch. https://pyimagesearch.com/2017/04/03/facial-landmarks-dlib-opencv-python/
14. Beltrán, M., Calvo, M.: A privacy threat model for identity verification based on facial recognition. Comput. Secur. 103324 (2023)
15. Saraswat, D., Bhattacharya, P., Shah, T., Satani, R., Tanwar, S.: Anti-spoofing-enabled contactless attendance monitoring system in the COVID-19 pandemic. Procedia Comput. Sci. **218**, 1506–1515 (2023)
16. Parveen, S., Ahmad, S.M.S., Hanafi, M., Adnan, W.A.W.: Face anti-spoofing methods. Curr. Sci. 1491–1500 (2015)
17. Ku, H., Dong, W.: Face recognition based on mtcnn and convolutional neural network. Front. Signal Process. **4**(1), 37–42 (2020)
18. Nguyen, H.V., Bai, L.: Cosine similarity metric learning for face verification. In: Kimmel, R., Klette, R., Sugimoto, A. (eds.) ACCV 2010. LNCS, vol. 6493, pp. 709–720. Springer, Heidelberg (2010). https://doi.org/10.1007/978-3-642-19309-5_55
19. geeksforgeeks. https://www.geeksforgeeks.org/eye-blink-detection-with-opencv-python-and-dlib/
20. da Rosa Righi, R., et al.: Designing Cloud-Friendly HPC Applications. In: Borin, E., Drummond, L.M.A., Gaudiot, J.L., Melo, A., Melo Alves, M., Navaux, P.O.A. (eds.) High Performance Computing in Clouds, pp. 99–126. Springer, Cham (2023). https://doi.org/10.1007/978-3-031-29769-4_6
21. Tomar, A., Kumar, S., Pant, B.: Crowd analysis in video surveillance: a review. In: 2022 International Conference on Decision Aid Sciences and Applications (DASA), pp. 162–168. IEEE (2022)