International Journal for Multidisciplinary Research (IJFMR)
E-ISSN: 2582-2160 ● Website: www.ijfmr.com ● Email: editor@ijfmr.com

Facial Frontiers: Unveiling the Potential of LBPHs and Haar Cascades in Facial Recognition for Enhanced School Security

Krish Goel[1], Meghna Das[2], Aastha Kumar[3], Godavari Tanmayi[4], T Suraj Kumar[5], Dr. Suganya R[6], Dr. Subbulakshmi T[7]

[1,2,3,4,5]Student, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India
[6]Faculty Supervisor, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India
[7]Faculty Co-Supervisor, School of Computer Science and Engineering, Vellore Institute of Technology, Chennai, India

Abstract
The article aims at introducing a Facial Recognition School Security System as one solution to improve security while speeding up administrative processes in educational institutions. The need for such a system emanates from concerns over the safety of schools as well as inadequacies inherent in conventional attendance and access control methods. Inadequate methods can be manual or rely on an older technology that leads to inefficiencies, inaccuracies and breaches of security. This proposed solution exploits contemporary artificial intelligence algorithms and computer vision techniques to facilitate the reliable identification and validation of entrants thereby providing contactless approach during Pandemic times in compliance with the COVID-19 safety protocols. At this period of COVID-19 it also acts as an avenue where physical touchpoints are reduced with consideration to social distancing measures. Our method is novel in the fact that it only detects and recognizes human faces as opposed to general object detection systems. We use Local Binary Pattern Histograms (LBPH) for face recognition and Haar Cascades for face detection. The Haar Cascade algorithm employs simple rectangular features to detect faces, using a cascade of weak classifiers to achieve high detection rates. The LBPH algorithm captures local texture patterns of facial features, calculating LBP values for each pixel. Our project demonstrates variable performance across different classes, with precision ranging from 0.50 to 1.00, recall from 0.33 to 1.00, and F1 scores from 0.33 to 0.94, while achieving an overall accuracy of 0.75, indicating robust performance in certain scenarios but room for improvement in others.

Keywords: Facial Recognition, School Security System, Artificial Intelligence, Computer Vision, COVID-19, Local Binary Pattern Histograms, Haar Cascades, Accuracy

1. Introduction

New technologies and mechanical advancements have resulted in a fast-changing education environment, which demands constant efforts to secure students as well as faculty members. However, the methods that

have been used to tackle existing security threats like physical violence and unauthorized access are mostly traditional and thus not able to respond in real-time. The paper therefore suggests creating a School Security System that is based on contemporary computer vision and facial recognition technologies in order to make safer learning environments.

The threats to schools have increased dramatically today. Some of these are violence, trespassing, or weapon possession which highlight the inadequacy of age-old strategies like ID cards and manual attendance registers. Such methods are not only slow but also subject to human slip-ups and fraud. On top of all these issues is the fact that there are numerous COVID-19 related health measures being implemented by schools around the world necessitating changes in their ways of enhancing security.

The emergence of Computer Vision and Facial Recognition provide new hopes in this regard. The use of this technology to precisely identify people has gained significant interest in sectors such as the law, banking and personal devices development. Our desire is to create a seamless, automated system that uses real-time identification and verification through integrating this technology into a school security system. Apart from that, it hardens the access control mechanism as well as preventing illegal entry to create a safer place for all people.

This plan aims at automating security systems' identification process in order to remove human errors by reducing manual checks. These are special cameras that capture images of people who visit schools. After being processed these images are compared with the registered list of students' names. Once identified successfully one is given permission while in case of failure it communicates to security personnel who have an intruder at hand.

Additionally, besides improving security, this system wants to enable efficiency in some administrative processes including tracking attendance. This means that each student's time logging can be automatically done by the system leading to accurate attendance.

To realize these aims, the project combines algorithms with software tools:

- **Face Identity Detection Algorithm:** Local Binary Pattern Histograms (LBPHs) is used in face recognition. LBPH is a robust and computationally efficient algorithm that can be used for real-time applications due to its low computational cost.
- **Computer Vision with Haar Cascades:** In object detection there's Haar cascades, a type of machine learning classifier. This enables the system to identify weapons or suspicious objects for increased security measures.
- **Programming Tools:** Facial Recognition and Computer Vision are built on open-source libraries like OpenCV. The facial data with access logs are stored in a secure database management system while the user interface makes it easier for administrators to run the entire system efficiently.

More so, this process should consider new parameters as a result of COVID-19 pandemic. The system design will enable potential integration with thermal cameras aimed at identifying people having high body temperatures that may be indicative of fever symptoms. Moreover, facial recognition could be deployed to monitor wearing of masks thereby ensuring adherence to safety protocols within school setting.

To sum up, the Facial Recognition School Security System stands out as a futuristic answer to the security issues of today. By merging complex technology with hands-on practices, this study seeks to make schools safer and more secure, providing assurance for scholars, parents and teachers among others.

2. Problem Statement

Educational institutions face numerous challenges in trying to maintain a safe environment and effective administrative procedures. Regularly, attendance and identification tracking methods are manual, tedious, prone to errors and cannot offer real-time monitoring. Additionally, conventional access control systems may be vulnerable to hacking or security breaches. For that reason, there is need for an automated solution that will effectively address these issues with respect to school security at large.

3. Related Works

Facial recognition technology has been widely studied and employed in security/ surveillance systems among other fields. Numerous researches have led to the development of pioneering face detection techniques as well as cutting-edge face recognition algorithms encompassing feature extraction. Viola and Jones [1] worked on one of the initial works on object detection including such facial detection. This method introduced cascade classifiers utilizing Haar-like features meaning that real time object detection could now be achieved; however, it is not perfect for dim lighting conditions or when the faces are partly obscured even though it worked efficiently computationally-wise.

Ahonen et al. [2] proposed the application of Local Binary Patterns on face recognition with textural features. While this strategy is computationally efficient and invariant to changes in illumination, it can become easily disturbed by large variations in pose or occlusions. For example, the Histograms of Oriented Gradients descriptor was applied for the first time in face recognition and pedestrian detection tasks by Dalal and Triggs [3]. HOG features are good for recognizing things because they model their local appearance and shape information. Even so, they may not work well when there is rotation or scaling. In the area of appearance-based face recognition, Turk and Pentland [4] presented Eigenfaces that represent faces as a linear combination of eigenvectors derived from a principal component analysis of face images. While it can be effective under controlled conditions, such systems might fail to operate properly if light intensities change abruptly or if postures change resulting into partial obstructions to the image formation process. However, Belhumeur et al. [5] introduced the Fisher faces technique by which a subspace minimizing within-class scatter while maximizing between- class scatter is determined using linear discriminant analysis. At times, this method may work better than Eigenfaces but it can again be problematic somewhere when the imaging circumstances alter.

To address face hallucinations, Liu et al. [6] proposed the two-stage approach. It comprised of a block which used a nonparametric approach at the local level and another block which used a parametric approach at the global level. In this case, face recognition systems should possibly stand to gain given that it is possible to get high-quality, facial images from low-quality input. In more complex cases, when the faces under consideration greatly deviate from the faces represented in the training set, the performance might be lower. For unconstrained face recognition, in which faces are photographed from a free environment, with variations in lighting, pose and occlusion, the lead worker, Zhou and Chellappa [7]. To address these issues, they proposed approaches to feature representation, matching, and, classification. While these techniques might hold future potential and may solve the current challenges and issues, they may still fail when it comes to handling large variations or poor input image quality. Yang et al. [8] proposed a dictionary learning method using Fisher discrimination for a sparse representation-based face recognition. This means that by incorporating class label information, this work aims at finding discriminative dictionaries which will in a way enhance recognition rate. This approach though may be highly computational and scalable for large-scale application may be challenging.

While these studies have pushed progress in facial recognition technology, their safety might be challenged with regard to accuracy, efficiency, or flexibility to potential variations in real-life situations. It is still challenging work and requires more research and advancements to eradicating the above-mentioned flaws and implement the facial recognition system and other security and managerial facilities in a systematic school security system.

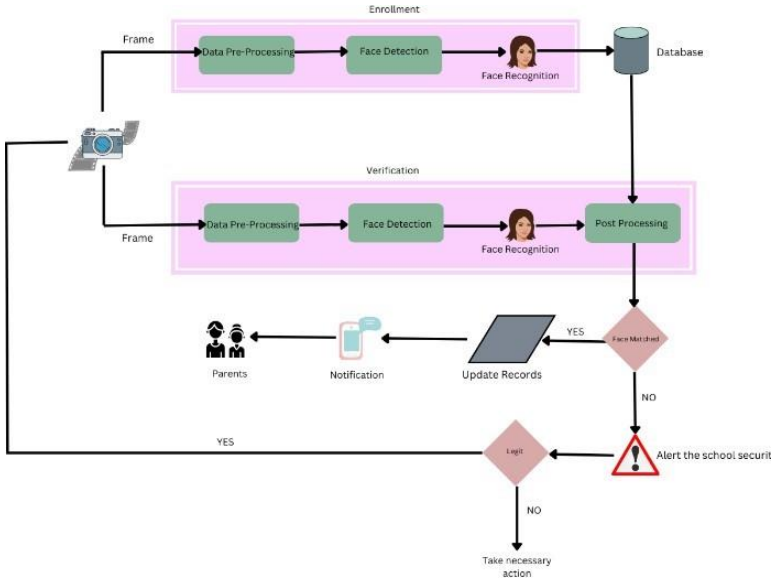
4. Objective

- Develop a comprehensive school security system incorporating facial recognition.
- Improve monitoring and automation of various tasks.
- Streamline attendance tracking.
- Strengthen security measures across the organization.
- Reduce paperwork and clerical tasks.
- Provide educational organizations with a reliable and effective tool for their activities.

5. Implementation

A. Flow Diagram

Figure 1: Flow Diagram



Enrolment Process:

Take Picture of the Person's Face: To begin with, there is a need to take a photo of the individual to be enrolled in the system.

Frame: The captured image is preprocessed so that it could be reformatted for another execution.

Data Pre-Processing: There is still image preparation for identifying people's faces. These may comprise noise reduction, contrast correct, and normalizing procedures.

Face Detection: Then it monitors which face is in the frame and its position.

Face Recognition: Facial characteristics from the areas of the body that were detected are transformed into a set of data called the faceprints.

Database: The extracted face print is then matched against the face prints stored in a database of face prints, each face print labeled by a unique identification of the person it belongs to.

Verification Process:

Take Picture: An individual is captured or filmed with a request to confirm.

Frame: The captured image is formatted to facilitate the ensuing treatment process.

Data Pre-Processing: As in the case of enrolment, the image data goes through the face detection module.

Face Detection: The system recognizes the existence and position of the face in the frame of the picture/Low.

Face Recognition: Further characteristics of the face are then extracted from the identified face and then turned into a faceprint just like in case of enrolment.

Post-Processing: The second change could be a further analysis of the faceprint extracted from the verification image by the system.

Database: The faceprint on the verification image is matched with those on the database list.

Face Matched: If the face comparing process finds a match between the faceprint from the verification image and a faceprint in the database, then it has been successful in its function.

Yes: If there is a match it then enters the processing depending on whether it is on enrolment or verification mode.

Enrolment:

Update Records: Information on the person is then entered into the database.

Verification:

Legit: The verification system then proceeds to verify the individual, and if the system is in a verification mode and there is a match, the person is given access or in other cases they are confirmed to be genuine.

No: If there is no match then the actions that follows depends on the mode of operation of the current instance.

Enrolment: There are no steps if the person is not a part of the system yet as a client.

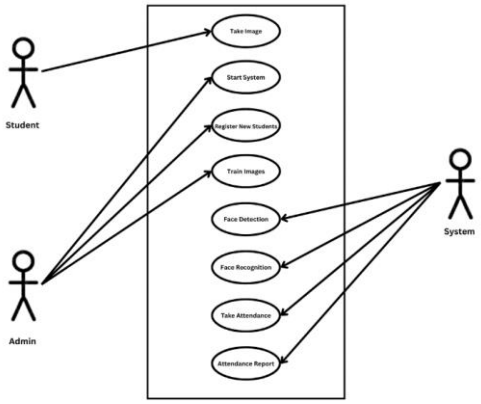
Verification:

Alert the School Security: Security staff is informed, by giving an alert of the reason as to why an outsider is trying to gain access to the compound.

Take Necessary Action: School security work based on their set, or known, responses to a threat.

B. Use Case Diagram

Figure 2: Use Case Diagram



The actor of the use case includes two actors and system for this project as shown below in the use case diagram.

Actors:

Student: The system user is the student who is lodging his/her attendance record in the registration system.

Admin: Under the admin level there are functions to add students and other duties such as managing the system.

System:

It is used as a system to aid in tracking a student's attendance. It is used in identifying the learners and this is done through using facial recognition technology thus marking their attendance.

The system initiates the facial recognition procedure. The student interacts with the system by signing to the camera, or in other words, the main gesture the student makes towards the system is through facial recognition. It takes a facial image and tries to input it into the student database that it has with this school. This we see, is because the system is able to pick a face in the captured image. Then the system uses facial recognition feature to attempt to match against the student in this image. If it successfully captures the student, it displays a label in the format of name roll no. department of the student. It also helps them to sign this label and if the machine is unable to identify the student, it will display the 'Unknown' label and the attendance of that person is not recorded.

C. Software Implementation

Graphical User Interface (GUI) Implementation: It will use the Tkinter library to create the GUI for setting up of various parameters for the facial recognition algorithm and the output will also be displayed here. The GUI consists of:

Coordinate System Specification: It is as follows: In defining the positions of GUI elements such as the size of the display window, the coordinate system is used depending on the implementation of the programming language; for instance, the X-coordinate.

GUI Components: Tkinter as a tool for creating GUIs is applied properly by selecting the proper methods to create a textbox, title, or button – that can interact with the system by the user.

Event Handling: Three Tkinter event handling methods are used to describe the operational characteristics of the system when user events trigger GUI elements.

D. Facial Recognition Algorithm Implementation

Face Detection Algorithm (Haar Cascades): OpenCV in combination with Cascade Classifier can be used to identify the presence of a face in the image, as well as finding its coordinates according to the layout of the GUI below.

Face Recognition Algorithm (Local Binary Pattern Histograms): This algorithm extracts the input image and feeds it to the facial recognition model that takes this vector as input. This model grosses out the crucial features of the face which are used in its recognition.

Algorithm Output Specifications: The visual layout formatting techniques which are employed in GUI framework are used to format the algorithmic forecasts returned by the prediction algorithm for interface rendering (for instance, transformation of detected faces into rectangles according to the GUI layout).

These specifications allow for the real time interaction of facial recognition prediction, operating on the algorithms on the GUI layout, and the relevant visualizations together with the packing methods defined.

E. Dataset and Preprocessing

Our project utilizes the "OpenCV – Facial Recognition – LBPH" dataset from Kaggle. This dataset has images of people from different ethnicities, genders and age groups. Images have variations in pose, lighting and facial expressions which are similar to real world scenarios we encounter during attendance marking. All images are 450x450. This so the data fed into the facial recognition model is the same. Then images are converted to grayscale. This reduces the computational load during feature extraction as grayscale images only require 1 channel v/s 3 channels in RGB images. Haar–like features are extracted from the preprocessed images. These rectangular features help to identify specific patterns in an image which corresponds to facial features like edges and lines. This is required for landmark localization in the faces. LBPH divides each image into small regions and for each pixel in a region, a binary string is generated based on the comparison of its intensity value with its neighboring pixels. The LBP histograms of all regions in the image form a feature vector which represents the spatial distribution of these local patterns. These LBP features are then used by the facial recognition model to distinguish between different people.

6. Research Methodology

The School Security System using Facial Recognition involved a thorough and systematic research methodology with various phases and techniques. The methodology was to ensure the system is accurate, reliable and practical to enhance school security. The key stages are as follows:

A. Requirements Gathering and Feasibility Analysis

In this stage, requirements for the school security system were gathered through series of consultations with stakeholders, school administrators, security experts and end-users (e.g. teachers, staff). A feasibility study was conducted to determine the technical feasibility, resource requirements and benefits of implementing a facial recognition - based security system in educational institutions.

B. System Design and Architecture

From the gathered requirements and feasibility study, a system design and architecture were developed. This involved defining the software components, selecting facial recognition algorithms (e.g. OpenCV) and integrating them with access control, attendance tracking and real-time monitoring. The system architecture also considered scalability, data security and user interface design.

C. Development and Implementation

In this stage, core facial recognition algorithms were developed and implemented. The activities on face detection, feature extraction, and recognition involved writing and testing of code. This module utilized open-source libraries and frameworks like OpenCV, modified them further for requirements in the school security system, and developed algorithms like LBPH and Haar Cascades for access control and attendance tracking, then integrated them with the facial recognition module.

D. Database Development and Integration

Our project uses a relational database management system designed and managed using MySQL Work-bench. All the student information is maintained in one table "Student" with the following attributes:

Table 1: Student

Attribute Name	Data Type	Description
Student_id	Varchar(45) (Primary Key)	Unique Identifier for each student
Name	Varchar(45)	Student's full name
Division	Varchar(45)	Student's class division
Roll	Varchar(45)	Student's roll number
Gender	Varchar(45)	Student's gender
Dob	Varchar(45)	Student's date of birth
Email	Varchar(45)	Student's email address
Phone	Varchar(45)	Student's phone number
Address	Varchar(45)	Student's city of residence
Teacher	Varchar(45)	Student's class advisor name
Dep	Varchar(45)	Student's academic department
course	Varchar(45)	Student's current course enrollment
Gender	Varchar(45)	Student's gender
Dob	Varchar(45)	Student's date of birth
Email	Varchar(45)	Student's email address
Year	Varchar(45)	Student's year of study
Semester	Varchar(45)	Student's current semester
Photo Sample	Varchar(45)	Student's photo sample present or not

The size of each student image stored is 450x450 pixels.

E. User Interface Design and Development

Design and development of the user-friendly interface for system administration, user registration, access logs, and alert monitoring are to be done. The principles relating to usability, accessibility, and intuitive design will enable the smooth running of the user experience. This interface shall be developed in Tkinter

or other relevant framework; it shall be integrated with facial recognition algorithms, similar to database components, to ensure smooth running.

F. Testing and Validation

These testing and validation processes have been carried out to provide every guarantee that the system is accurate, reliable, and effective under real-world scenarios. Unit testing enabled checking of the separate software modules or blocks of code; integration testing gave confidence in how all those various system components could interoperate. It targeted users, including real school administrators and teachers, to test usability, functionality, and overall efficiency in practical settings at large. Changes and enhancements that were necessary based on feedback from users and test results were applied.

G. Pilot Deployment and Evaluation

The system was then launched in a pilot phase usually within schools or selected educational institutions for personal testing and validation. During the piloting phase, the performance of the system was followed up, and feedback from users and other relevant stakeholders was elicited. Essential refinement and optimization, based on the assessment results, were carried out to ensure the functionality of the designed system and realize any limitations associated with the developed system.

H. Performance Analysis and Optimization

It performs a comprehensive performance analysis, including system accuracy, efficiency, and scalability evaluation. Among the parameters measured and analyzed are facial recognition accuracy rates, processing time, and system throughput. In this regard, various factors were taken into consideration which affect performance: light conditions, the quality of cameras, and dataset size. Optimization techniques were applied based on the analysis to improve the general performance of the system, to solve bottlenecks in the system, and to address limitations.

I. Documentation and Reporting

The process maintained detailed documentation with regard to design specifications, algorithm implementations, test cases, and performance analysis results. Thereby giving transparency, reproducibility, and any future enhancement or adaptation of the system. The research findings, methods used and the outcome would normally be compiled into a comprehensive report and presented at relevant conferences or published in journals of repute.

In the development of the School Security System with Facial Recognition, clear adherence to rigorous scientific principles and industry best practices has been followed. It combined theory analyses, practical implementations, and iterative refinement to provide a robust solution for enhancing the security measures at the school using facial recognition technology.

7. Algorithm Used

A. Haar Cascades

Haar Cascades use Haar-like features, which are basically the digital image features used for object detection in an image or video. It is said that features are computed based on the sum of pixel intensities taken in adjacent rectangular regions and by calculating their difference. Integral images are the intermediate representations used by Haar cascades in efficiently computing Haar-like features. The Haar

Cascades use a Cascade classifier, where each classifier is trained and their successive stages focus on the rest of the objects that go through. The face detection module in our project utilizes the Haar Cascades algorithm, which offers outstanding speed performance under such requirements, allowing even real-time face detection on devices with limited computational resources.

On the other hand, it has high performance in highly controlled scenarios with relatively constant illumination and face angles, typical in a school's entrance. Cascade structure of the algorithm makes it efficient to quickly reject non – face regions. Haar cascade quickly scans input images or streams of video and detects probable face regions. These detected faces would be passed onto the LBPH algorithm for recognition.

There are simple rectangular patterns that are used to detect specific characteristics in an image. These are known as Haar – like features. These features consist of adjacent rectangular regions with contrasting shades – "White Area" and "Black Area". White Area is the lighter region of the Haar-like feature while the Black Area is the darker region of the Haar-like feature.

$$f = \sum(\text{pixels in white area}) - \sum(\text{pixels in black area})$$

The feature value 'f' is the difference between the summation of pixel intensities in the area marked white and that of pixel intensities in the area marked black. Such difference may specify contrasts in the image that can define the existence of certain facial features such as edges, lines, and other patterns.

For weak classifier,

$$h(x) = 1 \text{ if } pf(x) < p\theta$$

h(x): Weak classifier function
x: Represents input which is a sub window of the image being analyzed
f(x): Feature value calculated for the input x using Haar- like feature
p: Polarity
ɵ: Threshold value
This formula allows the weak classifier to make a binary decision based on a single Haar-like feature. Multiple such weak classifier combinations are used to build a strong classifier in Haar Cascade algorithm.

B. LBPHs (Local Binary Pattern Histograms)

LBPs, Local Binary Patterns, is a texture operator that derives a binary number by locally thresholding the adjacent pixels. We chose the Local Binary Pattern Histograms algorithm due to the fact that it was robust against changes in illumination for the facial recognition feature in our application. Compared to some other algorithms, LBPH is not as sensitive to changes in lightning conditions. This may particularly help in a school environment where lighting changes over the day and around different areas of buildings. The other reason is related to the relatively lightweight computational requirements of LBPH. LBPH does well with a relatively small number of images per person. This is very critical in a school system where we have few images of each student. In our implementation, once Haar Cascade detects a face, it is analyzed by the LBPH algorithm against stored patterns in our database.

$LBP(xc,yc) = \sum(i=0 \text{ to } 7)\ s(gi-gc) \times 2^i$

(xc,yc): Coordinates of the central pixel being examined
gi: Gray level of a neighboring pixel
gc: Gray level of central pixel
s(x): Step function, s(x) = 1 if x >= 0 or 0 if x < 0
i: Index of the neighbor pixel
This formula calculates the LBP value for a single pixel by comparing it to its 8 neighbors. It creates a binary pattern based on whether each neighbor is brighter or darker than the central pixel. The LBP operator captures local texture information for facial recognition as it represents facial features like edged, spots and flat area.

$K(k) = \sum(i,j) \times I(fl(i,j) = k),\ k = 0,\ldots,n-1$

H(k): Histogram value for bin k
n: Number of different labels produced by the LBP operator
I: Indicator function
fl(i,j): LBP label for pixel at coordinates (i,j)
k: Bin index in the histogram (0 to n-1)
The histogram summarizes the texture information of the face, creating a compact representation that can be used for comparison and recognition.
Haar Cascades and Local Binary Pattern Histograms were way older than the more recent deep learning algorithms of facial recognition. These techniques are used in our project for a couple of reasons:

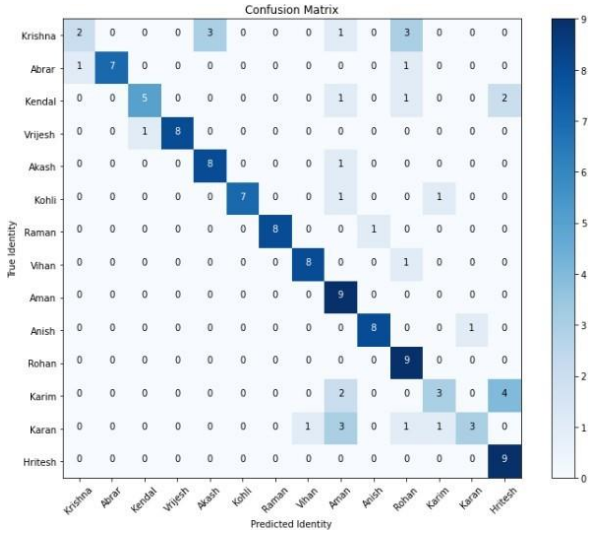
- **Resource Efficiency:** Haar cascades, LBPH require a lot fewer resources for processing and memory compared to Deep Learning models. Most of our system works in real-time on regular school hardware.
- **Faster Processing:** In our model implementation, Haar Cascades and LBPH are faster at processing than more complex Deep Learning models without a loss in accuracy that is notably significant.
- **Fewer Dataset Requirements:** Most of the schools would have limited facial data of students or staff working; facial data is personal in nature. LBPH works well even when the number of training images per class is relatively small compared to most deep learning models; hence, it would turn out to be more practical for our target environment.
- **Easy in Use and Maintenance:** Their relative simplicity makes them more feasible to implement and maintain by school IT persons who may have little or no experience with more advanced Deep Learning.
- **Privacy Issues:** The fact that LBPH stores only patterns, not real pictures, goes well with the strict data protection requirements usually in force in educational institutions.

While realizing the heavy outfitting that deep learning algorithms have in very challenging scenarios, our solution represents a balanced approach that suits certain needs and constraints of school environments. It offers a practical, efficient, and privacy-conscious solution that fits within schools with a shortage of resources.

8. Results and Discussion

A. Confusion Matrix

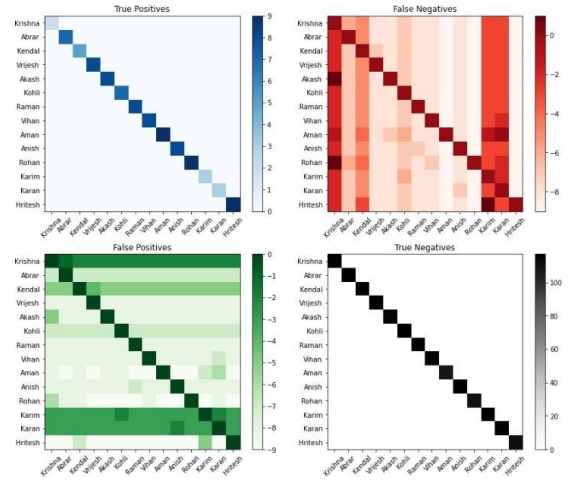
Figure 3: Confusion Matrix



It is a matrix where the rows represent the true identities, columns are the predicted identities, and diagonal elements are the number of correctly predicted identities for each class; and others are misclassifications. The elements on the diagonal, in blue, indicate the correct predictions for each class of identity. It correctly classified 'Aman' 9 times. The off-diagonal elements show misclassification. It misclassified 'Krishna' as 'Rohan' 3 times. Similarly, it misclassified 'Kendal' as 'Aman' once and as 'Kohli' once as can be seen from the row 'Kendal' at the intersection of the columns 'Aman' and 'Kohli'.

B. Performance Metrics Plot

Figure 4: Analysis of Performance Metrics

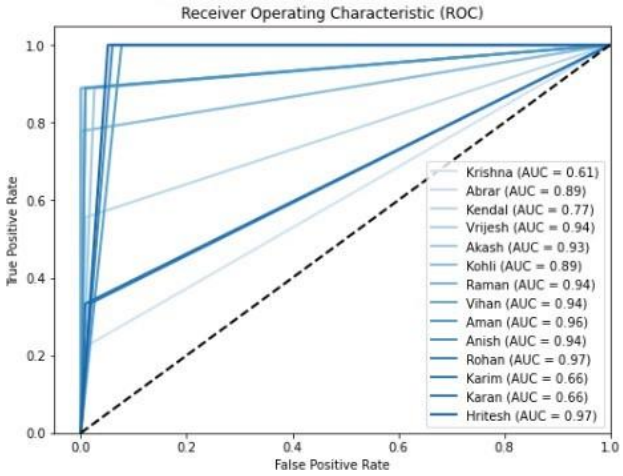


There are four independent bar plots in this diagram, each showing detailed classification performance for different identities or classes. Such plots will let one visualize the information about true positives, false negatives, false positives, and true negatives of a particular identity.

True Positives: The above bar plot represents the number of cases in a class that were correctly classified or identified. Higher bars indicate better performance for identifying those identities.
False Negatives: The above bar plot reflects the instances misclassified as belonging to a nonidentity when they should have been classified as belonging to that identity. The higher this plot is in its bars, the more misclassifications or missed detections it gives for that identity.
False Positives: This is a bar chart of the count of instances misclassified to belong to an identity they shouldn't belong to. The higher the bar, the more FP positive classifications for that particular identity.
True Negatives: This will be the number of examples correctly classified to belong to nothing in particular with respect to an identity; the higher the bar, the better the performance in correctly rejecting examples belonging to no given identity.

C. ROC (Receiver Operating Characteristic) and AUC (Area Under Curve)

Figure 5: Receiver Operating Characteristics (ROC) and Area Under Curve (AUC)



It is a ROC curve, a graph showing a model's performance with respect to binary classification at varying thresholds. This plots the True Positive Rate (TPR) versus the False Positive Rate (FPR) at a myriad of threshold values. The y-axis shows the TPR, and the x-axis shows the FPR. TPR is also referred to as sensitivity or recall; it is the proportion of actual positive cases out of all those that the model predicted as positive. The term is also referred to as the FPR, which defines the proportion of negatives in the cases that the model misclassified as positives. The various curves on this plot are for different classes or identities in the classification model. Now, it includes, in the legend, the AUC metric for each class. This is a summary demonstrating how the model performs: higher the AUC is, the better it classifies. A perfect classifier is represented with an AUC of 1.0 and an AUC of 0.5 refers to no better than chance performance by a random classifier.
This plot shows that class 'Hritesh' returns the highest AUC of 0.97, hence indicating excellent classification performance for this class, while classes like 'Karim' and 'Krishna' returned a pretty poor AUC value of 0.61, hence their poor classification performance. The ROC curve helps to draw competition between TPR and FPR for each single class. The top-left corner has good classification performance since this point maximizes the rate of true positives with a minimum false positive rate.

Analysis of the ROC curves, along with the respective values for AUC, yields insight into the strengths and weaknesses of the model in classification for different classes. This information may be useful in pointing out classes requiring further work or additional training data.
The ROC and AUC values of a binary classification model allow the assessment of its general performance and further provide insights into making informed decisions and model improvement.

D. Accuracy, Precision, Recall and F1-score

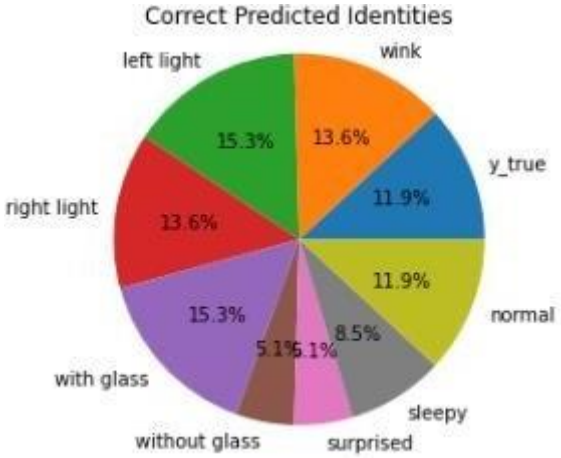
- Overall Accuracy = 0.75

Precision: Precision is the ratio of true positive predictions to the total positive predictions made by the model. It calculates the percentage of optimistic forecasts that come true.
Precision = True Positives (TP) / (True Positives (TP) + False Positives (FP))
Recall: Recall, also known as Sensitivity or TPR, is the ratio of true positive predictions to the total actual positive instances. It measures thefraction of actual positive instances that were correctly identified by the model.
Recall = True Positives (TP) / (True Positives (TP) + False Negatives (FN))
F1-score: The F1-score is the harmonic mean of precision and recall. It provides a single metric that balances both precision and recall, giving a better overall understanding of the model's performance. The F1-score ranges from 0 to 1, with 1 being the best possible value.
F1-score = 2 * (Precision * Recall) / (Precision + Recall)

Table 2: Precision, Recall and F1-Score by identities

Class	Precision	Recall	F1-Score
Krishna	0.67	0.22	0.33
Abrar	1.00	0.78	0.88
Kendal	0.83	0.56	0.67
Vrijesh	1.00	0.89	0.94
Akash	0.73	0.89	0.80
Kohli	1.00	0.78	0.88
Raman	1.00	0.89	0.94
Vihan	0.89	0.89	0.89
Aman	0.50	1.00	0.67
Anish	0.89	0.89	0.89
Rohan	0.56	1.00	0.72
Karim	0.60	0.33	0.43
Karan	0.75	0.33	0.46
Hritesh	0.60	1.00	0.75

Figure 6: Pie Chart on the distribution of correctly predicted identities



This is a pie chart of the various classes or categories for which the identities were Madison-distributed, where correct predictions are counted as instances. Every wedge corresponds to a sure class, its size proportionates to the number of those instances that were rightly predicted to belong to this class.
The classes represented in the pie chart are:

1. "Right light" (red slice): This class accounts for 13.6 % of the correctly predictedidentities.
2. "With glass" (purple slice): This class accounts for 15.3 % of the correctly predicted identities.
3. "Without glass" (violet slice): This class accounts for 5.1 % of the correctly predicted identities.
4. "Left light" (green slice): This class accounts for 15.3 % of the correctly predicted identities.
5. "Wink" (orange slice): This class accounts for 13.6 % of the correctly predicted identities.
6. "y_true" (yellow slice): This class accounts for 11.9 % of the correctly predicted identities.
7. "Normal" (light green slice): This class accounts for 11.9 % of the correctly predicted identities.
8. "Sleepy" (blue slice): This class accounts for 8.5 % of the correctly predicted identities.
9. "Surprised" (brown slice): This class accounts for 6.1 % of the correctly predicted identities.

From this pie chart, it can be noted that the maximum shares are by classes "Right light", "With glass", "Left light", and "Normal". These are the cases where the model was good at correctly predicting instances belonging to these classes.
On the other hand, "Without glass", "Sleepy", and "Surprised" have relatively small shares, meaning the model may have given way more mispredictions on instances from these classes.
The pie chart is one instant means of visualizing how well the model worked across different classes, thus showing in one glance the paths it performed very well or poorly in making correct predictions.

E. Discussion

This proposed system has many advantages over the traditional security measures in use at educational institutions. By automatization, this will put less burden on staff for access control and attendance tracking processes, reducing human error along the way—this improves efficiency. This provides real-time monitoring capabilities coupled with an alert system to enhance security through effective response time for probable threats or unauthorized access. These performance impacts result from several factors, including illumination variables, camera quality, and facial data size and diversity used for the training of recognition algorithms. Advanced techniques can remedy these limitations, most of which have the potential to provide solutions to further enhance accuracy and robustness of the system, also including

adaptive lighting compensation and transfer learning of facial recognition models. Moreover, there are risks of this technology to privacy and data security. Other future enhancement possibilities include the integration of extra biometric modalities for multi-factor authentication, and state-of-the-art anomaly detection algorithms detecting and raising a flag on suspicious activity. Cloud Computing and distributed architectures could combine to take this further in terms of sustaining the very much increased scalability of the system, giving way for possible seamless deployment across multiple educational institutions or campuses.

9. Conclusion

It estimates the potential of facial recognition technology within a school security system. The system shall utilize facial recognition to identify and verify a person for access control in all events, hence fully automating attendance tracking. At the development process, there was a deep literature review, follow ups with the stakeholders, rigorous designing and implementations, and testing for functionality. Performance analysis is very promising in terms of accuracy, efficiency, and scalability and seems to prove quite good viability for real-world applications. In having this system implemented, however, there is consideration to the limitations already existing within facial recognition technology: reduced performance due to unfavorable environments and concerns for privacy involving captured and used data continuously requiring improvements through enhancements of algorithms and techniques. If the School Security System with Facial Recognition proves implementable despite the challenges involved, security measures at schools could very well transform. This can help create a much safer environment to learn, teach, and visit for students, faculty, and visitors through easing some administrative processes and enabling real-time monitoring. It is also expected to cut down the burden of administration tremendously and make operations run smoothly. However, it still has to make sure that it takes care of the privacy and data security aspects. Strong encryption and compliance adherence will provide a way for using this system more responsibly and ethically. This finally ushers us to the conclusion: The School Security System with Facial Recognition presents a promising avenue likely to leverage cutting-edge technology in improving the security of learning facilities. On the contrary, this will open up more innovative ways of bettering such, leading to a safer and more secure learning environment.

10. Future Scope

Face Recognition algorithms are optimized to improve accuracy and speed when dealing with large datasets and real-time video processing. Smooth and fast face detection and recognition are made possible by the handling of real-time video processing, which makes the integration seamless when dealing with live video feeds. Real-time updates and notifications on attendance marking and system status instantly make one aware of security events. A mobile application to make attendance data and notifications accessible from any other place will enhance mobility and accessibility. Additional modalities can be added to the system—continuing with fingerprint or iris recognition—to provide higher security for the system and its reliability through multimodal biometric authentication. Research speech recognition as a method to provide security and usability through hands-free operation and user authentication. Introduce cloud computing to make it self-scaling and more accessible. Adopt a distributed system architecture to cope with the demand arising from multiple school campuses or institutions by having multiple recognition endpoints. Face mask detection can be integrated into the system to ascertain safety protocols for attendance marking procedures in a pandemic-stricken environment, like the one presently suffering

from COVID-19. Implement advanced algorithms for anomaly detection to flag suspicious activities and increase the security features of the system. Study migration to NoSQL databases like MongoDB, which have flexible schema and scale capabilities. Integrate IoT sensors to automate attendance marking based on physical presence at places of interest, reducing manual intervention. Integrate deep learning models, such as Convolutional Neural Networks, for probing the integration that gives way to more precise and robust face recognition. Develop a web-based interface to provide remote access to attendance records and system management, making it accessible and convenient. Set up automated testing, deployment, and update procedures with CI/CD pipelines; this will smoothen development and maintenance processes. Build in user feedback mechanisms that can improve the application based on user experience and evolving requirements. Factors that are identified here are the scope elements for further related research, development, and enhancement of the School Security System using Facial Recognition. Their mitigation will definitely contribute much towards performance, security, scalability, and user experience, ultimately making the system future-proof and quite effective to meet all requirements that an educational institution would lay down.

11. Acknowledgement

We would like to express our sincere gratitude to the Vellore Institute of Technology Chennai, for providing the SEED funding that enabled the design and development of the VITemp Detector: Entry Gate Access Control using Face Detection with Temperature Scanning.

References

1. Viola, P., & Jones, M. (2001). Rapid Object Detection using a Boosted Cascade of Simple Features.
2. Ahonen, T., Hadid, A., & Pietikäinen, M. (2006). Face Recognition with Local Binary Patterns.
3. Dalal, N., & Triggs, B. (2005). Histograms of Oriented Gradients for Human Detection.
4. Turk, M., & Pentland, A. (1991). Eigenfaces for Recognition.
5. Belhumeur, P. N., Hespanha, J. P., & Kriegman, D. J.(1997). Eigenfaces vs. Fisherfaces: Recognition using Class Specific Linear Projection.
6. Liu, C., Shum, H. Y., & Zhang, C. (2002). A Two-stage Approach to Hallucinating Faces: Global Parametric Model and Local Non-parametric Model.
7. Zhou, Z. H., & Chellappa, R. (2012). Unconstrained Face Recognition.
8. Yang, M., Zhang, L., Feng, X., & Zhang, D. (2010). Fisher Discrimination Dictionary Learning for Sparse Representation.