Table of Contents

[1. Introduction 1](#_Toc200472981)

[2. Problem Statement 2](#_Toc200472982)

[3. Objectives 2](#_Toc200472983)

[4. Methodology 3](#_Toc200472984)

[4.1 Requirement Identification 3](#_Toc200472985)

[4.1.1 Literature Review 3](#_Toc200472986)

[4.1.2 Requirement Analysis 4](#_Toc200472987)

[4.2 Feasibility Study 5](#_Toc200472988)

[4.2.1 Technical 5](#_Toc200472989)

[4.2.2 Operational 6](#_Toc200472990)

[4.2.3 Economic 6](#_Toc200472991)

[4.2.4 Schedule 6](#_Toc200472992)

[4.3 High Level Design of System 7](#_Toc200472993)

[4.3.1 Basic System Flow Diagram 7](#_Toc200472994)

[4.4 Description of Algorithm 8](#_Toc200472995)

[5. Expected Outcome 12](#_Toc200472996)

[6. References 13](#_Toc200472997)

# 1. Introduction

Attendance tracking is an essential administrative task in academic and professional institutions. Traditional methods such as roll calls and manual sign-in sheets are still widely used but are often inefficient, prone to human error, and easily manipulated. These methods consume valuable time, affect productivity, and compromise the integrity of attendance records. Studies have shown that institutions lose significant instructional or operational time due to outdated attendance methods. Moreover, the rise of proxy attendance where one individual marks presence on behalf of another, remains a widespread issue, particularly in classroom environments.

The global COVID-19 pandemic introduced additional challenges by making face masks mandatory in most public and institutional settings. This shift has rendered many conventional biometric systems ineffective, as facial features are partially obscured. Furthermore, advances in spoofing techniques such as printed photos or recorded videos have raised security concerns in automated systems, making liveness detection and anti-spoofing mechanisms more critical than ever [1].

In the context of Nepal, while certain institutions such as airports and telecom providers have implemented biometric or digital tracking systems, most universities and colleges still rely on manual attendance processes. These are not only outdated but also fail to scale with growing class sizes and health-conscious environments. There is a clear need for a smarter, contactless, and secure solution tailored for local academic institutions [2].

To address these challenges, our project introduces a Face Recognition Attendance System enhanced with mask detection and resistance to spoofing. The system leverages real-time camera feeds and advanced computer vision techniques to identify students accurately, even when wearing face masks. Anti-spoofing mechanisms such as blink detection and head movement tracking ensure that only live individuals are marked present, thereby reducing the risk of fraudulent entries. Attendance data is logged securely into both CSV files and an optional MySQL database for scalability and integration with broader academic management systems.

This project aims to provide a reliable, efficient, and secure attendance management solution that adapts to modern requirements while minimizing administrative overhead and improving accuracy.

# 2. Problem Statement

In educational institutes and workplaces, manual or traditional methods are still being used to track attendance. These traditional methods such as roll calls, sign-in sheets and ID card swipes are time consuming, prone to human error and vulnerable to fraudulent activities such as proxy attendance. A face recognition system can address these issues in attendance tracking. However the COVID-19 pandemic has introduced a new problem in the traditional face recognition system with the wide use of face masks. It reduces accuracy as well as increase the risk of spoofing attacks which tries to fool the system by using photos and videos.

Thus our system aims to create a web based face recognition attendance system that first begins with a core face recognition module and gradually adds features for mask detection and anti-spoofing.

# 3. Objectives

The primary goal of this project is to develop a robust and intelligent web-based Face Recognition Attendance System enhanced with mask detection and anti-spoofing mechanisms. The system aims to:

* To replace manual attendance systems with a real-time facial recognition-based solution using LPBH and OpenCV.
* To integrate a mask detection model and liveness detection techniques using Keras and dlib libraries, enhancing our system’s performance.

# 4. Methodology

For the development of the Face Recognition Attendance System with Mask Detection and Anti-Spoofing, we will adopt an Iterative Development Model. This approach suits our project well, as we are actively learning, experimenting, and refining features during development.

We will begin with the core face recognition module, then gradually add features such as mask detection, anti-spoofing (blink and head movement detection), and finally database integration. Each module will be independently developed, tested, and refined before moving on to the next, ensuring that the system remains functional and adaptable throughout the process.

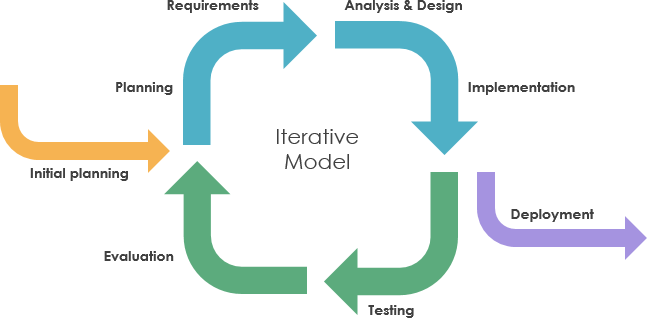


Figure 1: Iterative Software Development Model

## 4.1 Requirement Identification

Face recognition technology has advanced quickly, leading to its use in security, authentication, and attendance systems. To improve accuracy and prevent impersonation, modern solutions now include mask detection and anti-spoofing, especially in response to health and digital security concerns.

### 4.1.1 Literature Review

**Smart Attendance Systems (SAS)**

Systems like SAS use facial recognition to automate attendance marking. These are typically built with OpenCV and Haar Cascades or LBPH algorithms for face detection and recognition. However, many such systems are limited to basic recognition and fail to consider real-world complications like face masks or spoofing threats [3].

**SecurOS® FaceX**

SecurOS® FaceX is a commercial face recognition attendance system used in corporate environments. It supports real-time recognition and stores attendance logs on the cloud [4]. However, its reliance on consistent network access and commercial licensing can limit its accessibility for smaller institutions.

**Real-Time Mask Detection Models (MobileNet, ResNet)**

Following the COVID-19 outbreak, several open-source projects integrated real-time mask detection into facial recognition pipelines using CNN models like MobileNetV2 [5]. While effective, most of these systems focused solely on detecting masks, without connecting to larger attendance systems or databases.

**AI Thermal Scanners with Mask Detection (used in airports)**

Some high-end commercial systems, especially in airports or hospitals, integrate mask detection with thermal scanning and face verification [6]. However, these are hardware-intensive and not easily replicable in educational or budget-constrained settings.

### 4.1.2 Requirement Analysis

Requirement analysis focuses on determining the needs of a system. The purpose of this analysis is to ensure that the software or system meets the desired goals. This system enables users register their face, mark their attendance and view the attendance log as well.

1. **Functional Requirement**

Functional requirements define the core functions the system must perform to meet its purpose.

1. User Face Registration

* Administrators should be able to register user’s (students) face data through the system, which will be used for future identification and attendance tracking

1. Real-Time Face Recognition

* The system must detect and recognize registered users in real-time using a live camera feed.

1. View Attendance Records

* Users or administrators should be able to view daily attendance records.

1. Mask Detection and Anti-Spoofing Mechanism

* During recognition, the system should detect whether the user is wearing a mask correctly. Attendance may be flagged or denied based on the result.
* The system should prevent fake attendance through photos or videos by incorporating liveness detection methods like blink detection and head movement.

1. Database Integration

* All user data and attendance logs should be stored in a structured and persistent MySQL database.

1. **Non-functional Requirement**

Non-functional requirements define the quality and performance aspects of the system, ensuring it works efficiently and reliably.

1. Performance: Face recognition and mask detection should happen in real-time with minimal delay.
2. Security: The system should prevent fraudulent entries using liveness detection and secure data storage.
3. Usability: The interface should be user-friendly and intuitive for both technical and non-technical users.
4. Portability: The system should run on any desktops with minimal installation/configuration steps.

## 4.2 Feasibility Study

The purpose of the feasibility study is to consider all the aspects of the proposed project and determine its success. It also evaluates the project for its practicality. In this chapter we determine if we have the right technology, financial resources, and time required to complete the project and whether the project will be completed in time.

### 4.2.1 Technical

The required technologies such as Python, OpenCV, MySQL, and deep learning libraries (Keras, dlib) are readily accessible. The frontend and backend interfaces can be developed using MERN stack optionally, with core face recognition functionalities integrated through Python-based services. Also, hardware requirements are minimal, involving only a standard computer and a webcam, making our system technically feasible.

### 4.2.2 Operational

Our system is easy to use with a simple interface that allows users to perform key tasks like registration, attendance tracking, and dataset management with minimal training making the system practical and operationally feasible.

### 4.2.3 Economic

The system relies on open-source tools and libraries, reducing development costs significantly. It can run on standard computers without requiring high-end hardware or paid licenses. This cost-effective approach makes our solution affordable and hence, is economically feasible.

### 4.2.4 Schedule

The estimated duration of the project is around 2 to 3 months. Considering our team’s skills, the available resources, and the planned tasks, this timeline is realistic. By maintaining consistent monitoring and conducting regular progress checks, we can ensure timely completion so this is why our system is feasible in terms of schedule.

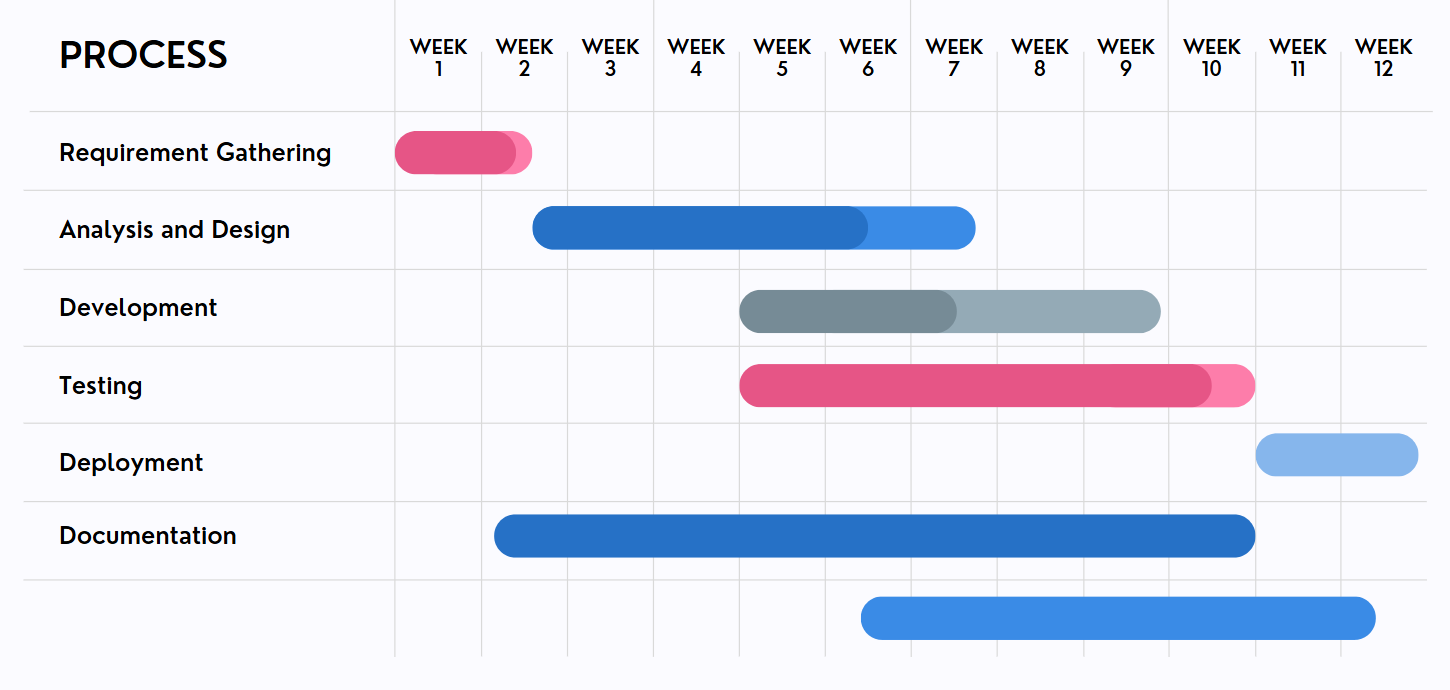
****

Figure 2: Schedule Gantt Chart

## 4.3 High Level Design of System

### 4.3.1 Basic System Flow Diagram

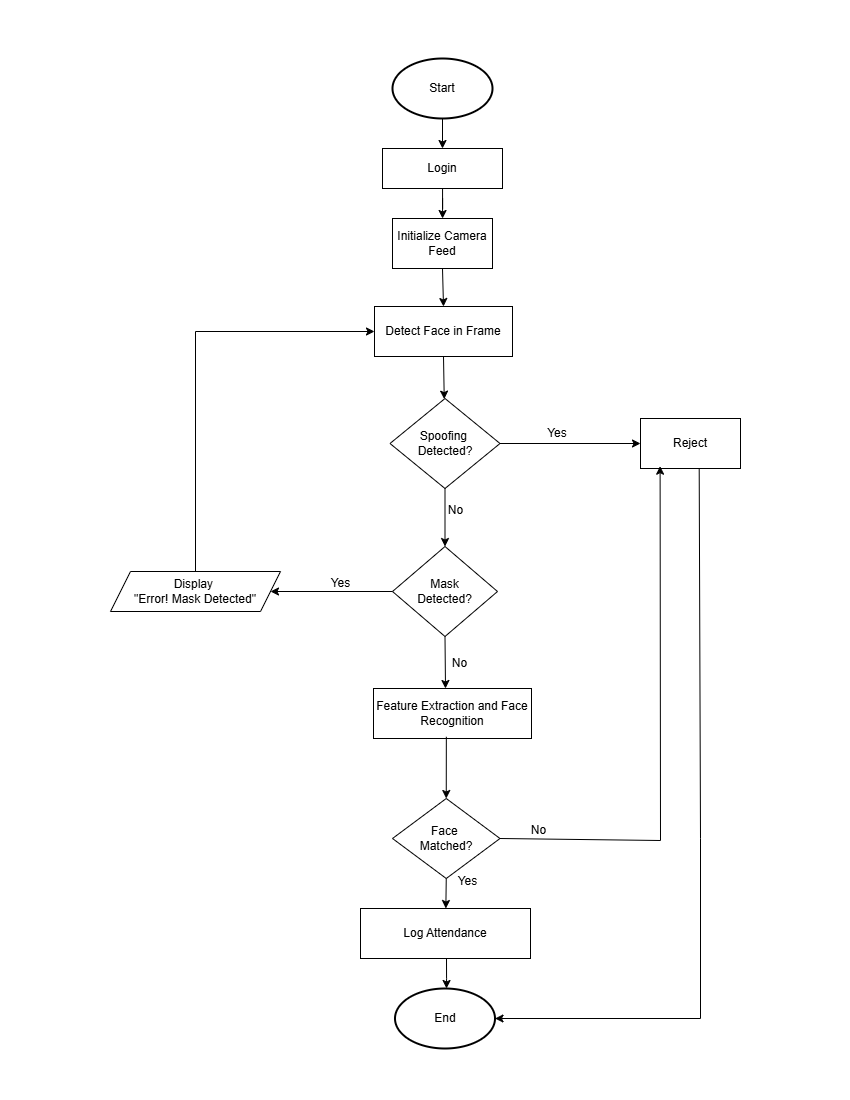


Figure 3: Basic System Flow Diagram

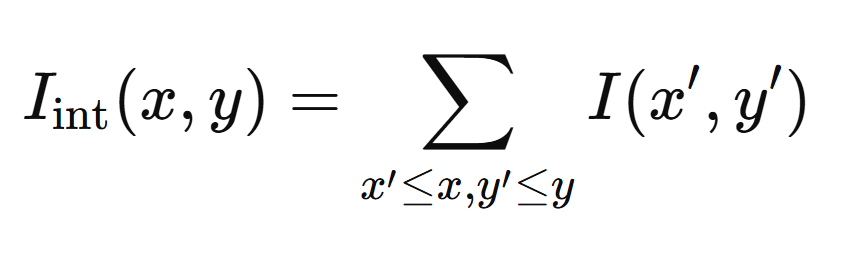
## 4.4 Description of Algorithm

This Face Recognition Attendance System utilizes a combination of computer vision and deep learning algorithms to ensure accurate recognition, even with masks and in the presence of spoofing attempts. The key technologies used are:

1. **Haar cascade classifier**

Haar cascades are machine learning–based classifiers used to detect objects, particularly faces, in images. This algorithm is based on the Viola–Jones object detection framework and uses Haar-like features to detect the presence of a face in an image. It scans the image at multiple scales and locations using trained classifiers, which are efficient due to the use of integral images and cascaded classifiers.

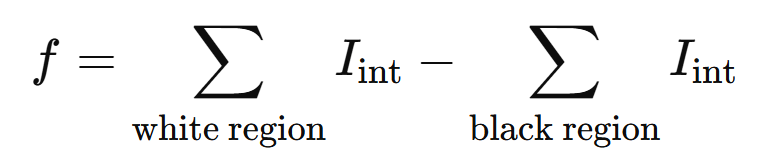
Integral Image:



Where I(x,y) is the original image intensity at pixel (x,y), and Iint(x,y) is the sum of all pixels above and to the left.

Feature Calculation:

A Haar-like feature ƒ is calculated as:



1. **LBPH (Local Binary Patterns Histograms)**

LBPH is a simple and efficient face recognition algorithm based on local texture features. It performs well in real-time applications and under varying lighting conditions.

LBPH Algorithm Steps:

1. Parameters

The LBP uses 4 parameters:

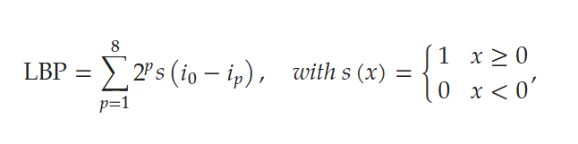
* Radius: Distance from the central pixel (commonly 1).
* Neighbors: Number of surrounding pixels (commonly 8).
* Grid X/Y: Divides image into cells (e.g., 8×8), increases feature detail and histogram size.

1. Training Phase

* Use a dataset of labeled facial images.
* Assign an ID (name or number) to each person’s images.
* These are used to build reference histograms.

1. Applying LBP
2. Convert the image to grayscale.
3. For each 3×3 window:

* Use the center pixel as the threshold.
* Compare each neighbor to the center:
* 1 if ≥ threshold, 0 if < threshold.
* Concatenate binary values into a string, convert to decimal.
* Replace the center pixel with this value.

1.  Result: A new image that emphasizes local texture patterns.

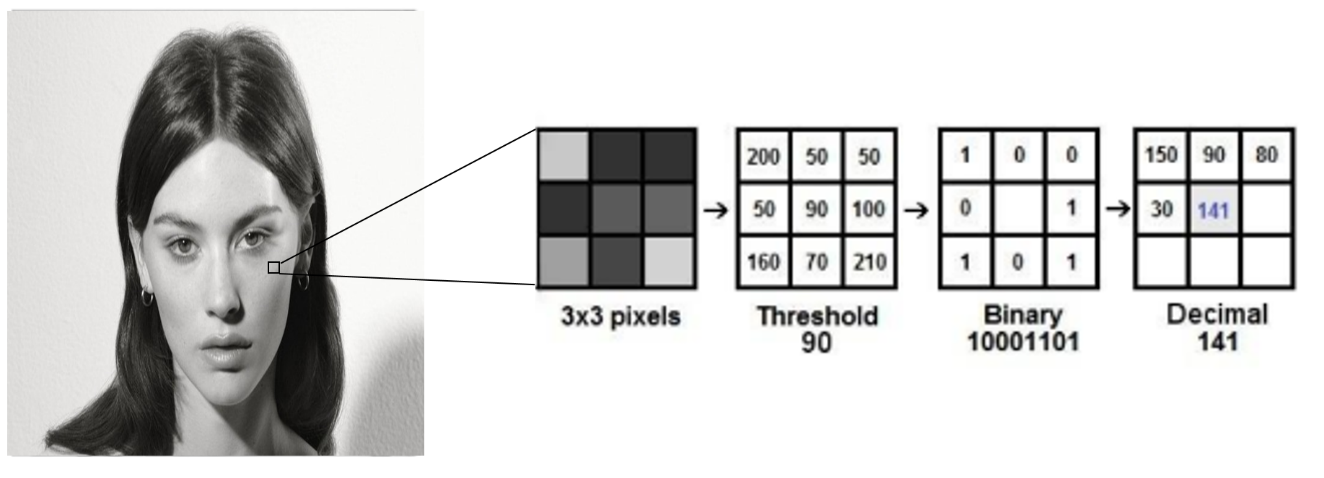
 where, 𝑖0 and 𝑖𝑝 are the intensity value of the center pixel and neighborhood pixels, respectively.

Figure 4: Facial Image in gray scale applying LBP operation

1. Extracting Histograms

* Divide the processed image into Grid X × Grid Y regions.
* For each region, compute a histogram (e.g., 256 bins for grayscale).
* Concatenate all region histograms into a single large feature vector.
* Example: 8×8 grid → 8×8×256 = 16,384 features.

1. Face Recognition
2. For a new image, compute its LBP histogram using the same process.
3. Compare the new histogram with those in the training set using:

* Euclidean Distance
* Chi-Square

1. The closest match (smallest distance) indicates the recognized person.
2. The matching distance can serve as a confidence score:

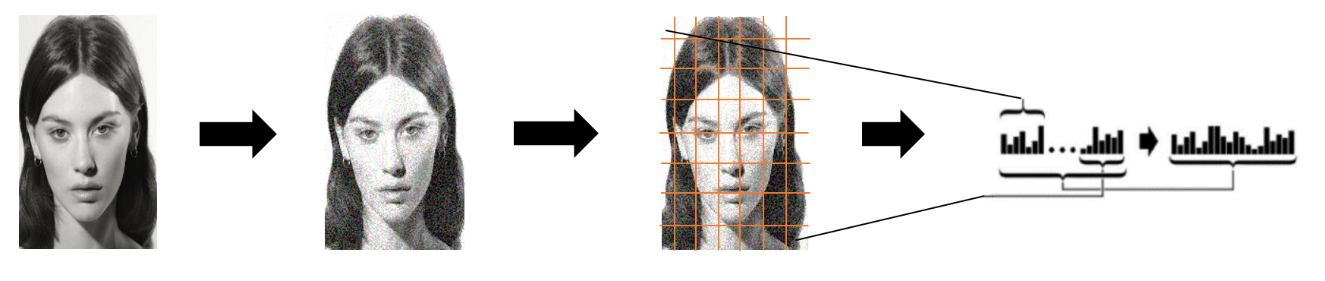
* Lower Score=better match
* Use a threshold to decide recognition success

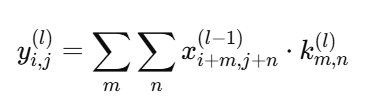
Figure 5: Histogram Extraction

1. **Convolutional Neural Networks (CNNs) binary classifier:**

A CNN binary classifier works by learning patterns from images to distinguish between two classes, such as:

1. Masked vs. Unmasked
2. Real Face vs. Spoof Face

Mathematical Components:

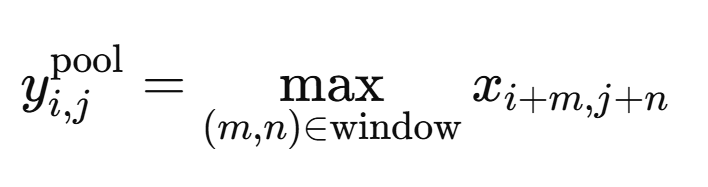
* **Convolution Layer:**

Where:

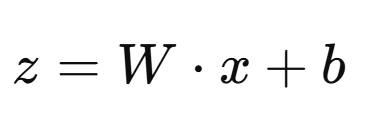
* x(l−1): input to layer l
* k: convolution kernel
* y(l): output feature map
* **Activation Function(ReLU)**

f(x)=max(0,x)

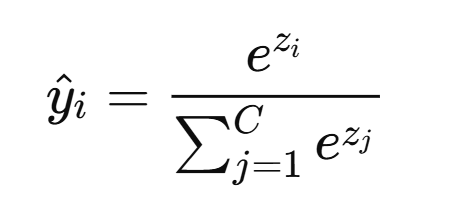
* **Pooling Layer**: Reduces spatial dimensions to speed up computation.



* **Fully Connected Layer**: Learns complex relationships and outputs predictions.



* **Softmax Function** (for final classification):



Training is performed on a labeled dataset of known student images, and the model is fine-tuned for best accuracy.

# 5. Expected Outcome

Upon completion, our system is expected to incorporate several key functionalities and features aimed at enhancing attendance management through face recognition technology.

First, it will include an automated attendance system that leverages face recognition to record attendance in real time, ensuring efficiency and accuracy. A mask detection feature will be integrated to identify whether a person is wearing a mask correctly. This feature can be configured to either flag or deny attendance to individuals not adhering to mask protocols.

To ensure the integrity of the attendance system, anti-spoofing mechanisms such as liveness detection like blink detection or head movement, which will be implemented to prevent fraudulent check-ins. A user-friendly interface will be developed, enabling easy student registration, live monitoring, and attendance viewing.

Additionally, the system will maintain accurate attendance logs, storing data in a structured format (such as CSV files or a database) with proper timestamps while preventing duplicate entries. Finally, the design will be expandable, allowing for future enhancements like deeper model integration or syncing with cloud services.

# 6. References

1. A. K. Jain, A. A. Ross, K. Nandakumar, “Introduction to biometrics,” in Handbook of Biometrics, Springer, pp. 1–22, 2011.
2. R. Pandey and S. B. Diyal, “A Study on Situation of National Identity Card in Nepal: implications and challenges,” *Educational Journal*, vol. 2, no. 2, pp. 10–26, Nov. 2023.
3. D. Saraswat, P. Bhattacharya, T. Shah, R. Satani, and S. Tanwar, “Anti-spoofing-enabled Contactless Attendance Monitoring System in the COVID-19 Pandemic,” *Procedia Computer Science*, vol. 218, pp. 1506–1515, Jan. 2023.
4. “SecurOS® FaceX | ISS · Intelligent Security Systems,” *ISS · Intelligent Security Systems*, Apr. 02, 2024. (accessed May 23, 2025).
5. P. Nagrath, R. Jain, A. Madan, R. Arora, P. Kataria, J. Hemanth, “SSDMNV2: A real time DNN-based face mask detection system using single shot multibox detector and MobileNetV2,” *Sustainable Cities and Society*, vol. 71, pp. 102964, Mar 2021.
6. A. Barnawi, P. Chhikara, R. Tekchandani, N. Kumar, B. Alzahrani, “Artificial intelligence-enabled Internet of Things-based system for COVID-19 screening using aerial thermal imaging,” *Future Generation Computer Systems,* vol. 124, pp. 119-132, Nov. 2021.