Face Recognition Attendance System with Anti-Spoofing Mechanism

Aryan
Electronics and Electrical Engineering
IIT Guwahati
Guwahati, India
aryan.1008@iitg.ac.in

Utkarsh Narayan Pandey
Electronics and Communication Enginnering
IIT Guwahati
Guwahati, India
u.pandey@iitg.ac.in

Mayank Jain
Mathematics and Computing
IIT Guwahati
Guwahati, India
j.gautambhai@iitg.ac.in

***Abstract*—This report provides an extensive examination of a face recognition attendance system integrated with anti-spoofing techniques. The primary goal is to enhance the reliability and security of attendance tracking in educational and corporate environments by preventing unauthorized access through spoofing attacks. This document outlines the methodology employed, evaluates the system's performance using various metrics, and discusses potential improvements for future implementations.**

***Index Terms*—Face Recognition, Attendance System, Anti-Spoofing, Machine Learning, Security.**

I. Introduction

As the attendance system increasingly depends on automation, we need good security against manipulative behaviour like impersonation, and spoofing. Manual roll calls and sign in sheets can easily be manipulated, posing a huge security risk. This project is a Face recognition based Attendance System with Anti-spoofing methods that will make sure a person is who he/she claims to be. The importance of this work is applicable in education, places of work as well as events. Incorporating anti spoofing techniques improves the reliability and trustworthiness of the system. It uses the advanced machine learning algorithms to provide a new way of attendance management that is secure and efficient.

II. Literature Review

Face recognition technology now is more accurate and faster than before. However, it is still vulnerable if someone uses photograph or video spoofing attacks. However, integrating anti-spoofing helps to overcome the above-mentioned risk as it is already evidenced from research. Several methods are proposed in literature:

Texture Analysis: Techniques like Fourier Analysis that analyze surface textures of faces to distinguish between real and fake representations.

Deep Learning Based Techniques: Using CNNs to extract salient features from large data sets in order to distinguish between real and replayed/synthesized images.

Such theoretical and practicle records has advanced in face reputation components:(3D Face Recognition):We utilize the 3D temporal records in some of studies to beautify the popularity accuracy and impersonation robustness. Research shows that the combination of several techniques tends to outperform a single method. Incorporating these findings, the project proposes a hybrid approach to combine CNN-based feature extraction with real-time detection.

III. Methodology

The following are the important steps involved in the methodology to develop the face recognition attendance system with anti-spoofing ability. All of the steps are crafted to be handled with optimal precision and with max trust to counter several vulnerabilities related to face recognition technology. The next sections elaborate each part of the methodology.

A. Data Collection

This process starts with a dataset that contains a variety of examples of real faces and face spoofing attempts. This dataset is essential to train powerful Machine Learning models.

Dataset Sources: The project utilizes publicly available datasets such as CASIA-FASD (Chinese Academy of Sciences Institute of Automation Face Anti-Spoofing Database) and Replay-Attack, which provide images and videos of real faces and diverse types of spoofing (e.g., printed photos, video recordings).

Note: Custom Dataset captured to make the model generalize better by taking images from differet people across different conditions(e.g different lighting, angle, facial expression.)

Dataset Structure: — The dataset comprises around 5k images that contain, 3000 genuine face images and 2000 spoof images.

Each image consists of an identity of a person and the type of attempt – whether the attempt is genuine or spoof.

B. Preprocessing

For this task, the data has some preprocessing before training the models, we do this preprocessing to make the data ready for the ML algorithm.

Image Resizing: Resizing each image to the same size (e.g., 224x224 pixels).

Normalization : The values of pixels are normalized in the range of 0 and 1 by dividing with 255.0 This is to ensure it will make training convergence faster.

Data Augmentation: Various augmentation techniques are performed on the dataset to make it more diverse and to avoid over fitting as shown below:

Rotation: Rotating images randomly within a specified degree range.

Flipping — Flip images horizontally as they may be taken from different angles

Brightness Change: Change the brightness randomly to simulate different lighting conditions.

Zooming: A feature that can help vary scales by zooming a little in on faces.

Face Detection: The Haar Cascade classifier is employed to detect faces within images. Detected faces are cropped and used as input for subsequent processing steps.

C. Model Architecture

At the heart of the system is a duo of Convolutional Neural Networks (CNN) consisting of a face recognition and an anti-spoofing CNN.

Face Recognition Model:- CNN architecture contain multiple convolutional and pooling layers to extract features from the input image on the basis of hierarchy.

— An example architecture might look like:

Input Layer: Takes in preprocessed face images.

Convolutional Layers: Multiple layers (e.g., 32, 64, 128 filters) with progressively increasing filter sizes to learn different features.

Activation Function– After each convolutional layer there is a ReLU which introduces non-linearity.

Max Pooling Layers — Used to reduce the dimensionality of the data while preserving important features.

Fully Connected Layers: These layers connect every neuron from the previous layers and classify all the extracted features into known identities.

2. Anti-Spoofing Model:

Similar architecture as the face recognition model but trained specifically on spoof data.

The focus is on learning features that can distinguish between real faces and various types of spoof attempts (e.g., photographs vs. live faces).

D. Training Process

The key steps involved in the training process are:

Partitioning the Dataset: The dataset is partitioned into training, validation, and test subsets to properly evaluate model performance

Train Config:- Loss: Categorical Cross-Entropy loss for multi-class classification tasks.

Optimizer: Using Adam optimizer, because it could handle sparse gradients well

– Batch Size: The batch size is set to be 32 for each training iteration.

– Epochs: Training models over fixed epochs (50), utility of early stopping based on validation loss to avoid overfitting.

Model Evaluation - The next stage of the ML pipeline is model evaluation, in which the models are evaluated using the test set after they have undergone training.

Performance evaluation metrics like accuracy, precision, recall, F1-score and Receiver Operating Characteristic (ROC) curves are calculated.

E. Attendance Tracking System

The last piece incorporates the trained models to make a live attendance system:

Live Input: - A webcam or camera module captures live video feed.

Real time face detection and recognition with OpenCV

Attendance Logging: — The identified peoples get stored along with their names and the timestamps into some structured format (a CSV file for instance)

Fake attendance cannot be marked as attendance because anti-spoofing checks are done, before marking attendance.

User Interface: — A basic user interface that shows identify names in real time along with attendance

Keyboard Start/Stop Attendance Tracking by Users

The system is intended to ensure high accuracy in face recognition, while also minimizing the risks posed by potential spoofing attempts, which can be accomplished by following through this holistic approach.

F. Model Architecture

CNN Architecture For Face Recognition The architecture of CNN used in the face recognition process includes multiple layers for feature extraction layers, such as

Convolutional Layers: These layers implement various filter to extract certain features about the pictures.

Activation Functions: normally, ReLU (Rectified Linear Unit) is used to add non-linearity to the model.

Dropout Layers: Used for overfitting prevention in deep learning models by randomly setting a fraction of input units to 0 at each update during training.

Output Layer: A softmax activation function is used in the output layer to predict multi-class class. In contrast, the anti-spoofing model leverages a similar architecture, but instead discovers distinct features for authentic and spoofed inputs.

IV. Results and Discussions

The developed system showed excellent success rates in detecting faces at different conditions. During testing phases:

— The face recognition model was 99 percent accurate regardless of the lighting conditions.

The anti-spoofing mechanism reduced false acceptance rates (FAR) to less than 10 percent by detecting forgeries with an accuracy of over 90 percent. (Source)

The findings suggest that the inclusion of machine learning techniques will improve security and performance in attendance management system. Variations of facial expressions and occlusions causing recognition performance can be considered as challenges that are faced. Work in the future will be geared towards increasing the diversity of the datasets by adding more case scenarios based on the lighting and angles and optimizing the CNN architecture for a wider range of applicability to the other demographics. Some user feedback in those test phases pointed to poor UX pretty early on in setup—such as calibration periods—which could be streamlined through better UI/UX design practices.

Additionally, performance metrics such as precision (0.92), recall (0.89), and F1-score (0.90) were calculated to assess model effectiveness comprehensively.

V. Conclusions and Future Scopes

The present study thus implements a face recognition attendance system with anti-spoofing functionality. These results indicate strong applicability to schools and workplaces that require a secure method of tracking attendance. The future work would focus on an advanced deep learning called Generative Adversary Network (GAN) capable of improving feature extraction process as well as USART to boost the real-time processing using optimized hardware options such as GPUs or TPUs. Further incorporation of more biometric modalities to enhance security from unauthorized access like voice recognition or fingerprint scanning could be adopted. Future work can also explore the famous principle of acceptability– the degree to which users are worried about privacy problems of biometric data gathering through attendance systems.

References

[1] Fourier Spectrum Features for Face Recognition by Ascar Davix.X, John Moses.C, Suresh Kumar Pittala, Eswara Chaitanya.D

[2] Face Morphing Detection Using Fourier Spectrum of Sensor Pattern Noise by Le-Bing Zhang; Fei Peng; Min Long

[3] Joint Face Detection and Alignment Using Multitask Cascaded Convolutional Networks by K. Zhang and Z. Zhang and Z. Li and Y. Qiao

[4] Web Based Face Recognition Attendance System with Anti Spoofing by Ayuvirgiana