Face Recognition Attendance System with Anti Spoofing

Contents

Introduction

Attendance of the employees in an organization can be marked using face recognition. Employee just need to appear in front of camera for registering his attendance. Usual spoofing of face recognition systems by showing photographs could be prevented using anti spoofing techniques using deep learning.

Business Requirement

This is an automated attendance management system. This system, is based on face detection and recognition algorithms, automatically detects the employee when he enters the office and marks the attendance by recognizing him.

Current System

Current system using biometric attendance marking system using automated fingerprint based attendance marking. Automated **fingerprint based attendance system** has replaced the annoying manual registers in many organizations. Fingerprint attendance machine has a reader that scans finger impressions of employees and determines whether they are identical to the previously stored records. If they are found identical, the attendance criteria for the verified employees are maintained accordingly.

The main drawback of this system is that some person may have difficulty in their finger prints being recognized if they have very tender skin on if their fingers are quoted with oil or any similar substance.

Proposed system

Face detection and recognitions are done by deep learning methods. Face detection also refers to the process by which humans locate and attend to faces in a visual scene. Caffe Model is used for face detection. Histogram of Oriented gradients (HOG) method is used to detect a face, face landmark estimation is used to obtain 68 face landmarks these embedding (measurements) are then compared to the 128 measurements of the known image and an appropriate result is produced. When a face is detected by the camera it checks the corresponding values of the current visible face with values stored in the file. If the values are a match, then the face is recognized and the name associated with that face is displayed. The result is stored in the database for further processing.

The HOG algorithm applies a ‘sliding window’ across the entire image. For every stage of the sliding window, an HOG descriptor for that region is calculated. The descriptor is then compared to a template using a trained model to determine if a person’s face is located in that region or not.

Next is to use Conventional CNN-based face anti-spoof approaches to detect spoofing in the image or video. **A spoofing attack** is an attempt to acquire someone else’s privileges or access rights by using a photo, video or a different substitute for an authorized person’s face. Attackers may present face spoofs (i.e., presentation attacks, PA) to the system and attempt to be authenticated as the genuine user. The face PA include printing a face on paper (print attack), replaying a face video on a digital device (replay attack), wearing a mask (mask attack), etc.

Technologies used

- Keras
- CNN
- HOG
- Caffe Model

Risks and challenges

Some of the risks and challenges faced are below:

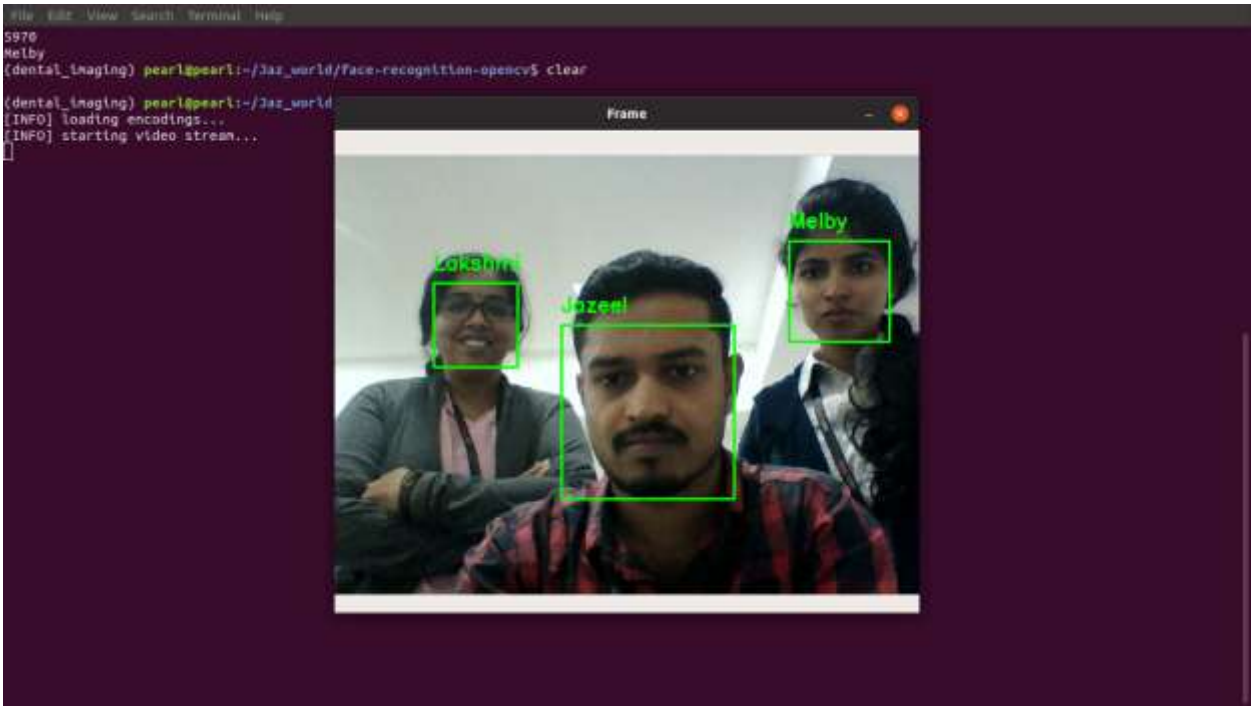
1. Required 100% accuracy for attendance marking

2. When the image is formed, factors such as lighting (spectra, source distribution and intensity) and camera characteristics (sensor response and lenses) affect to some degree the appearance of the human face.

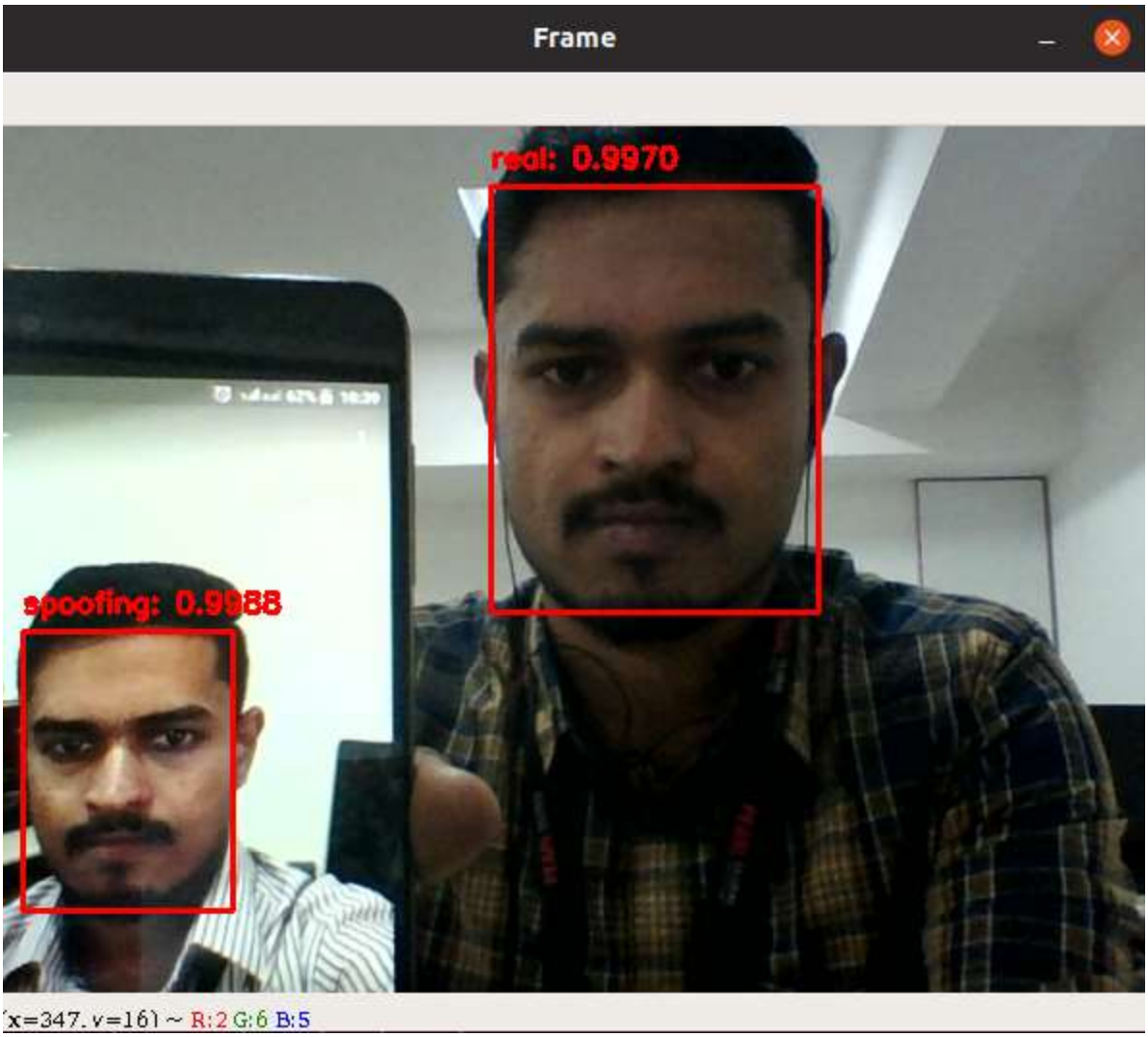
Examples of some challenges that may be existing in a human face

- Challenges because of illumination variations
- Challenges because of pose/viewpoint variations
- Challenges because of ageing variations
- Challenges because of facial expression/facial style
- Challenges because of occlusion

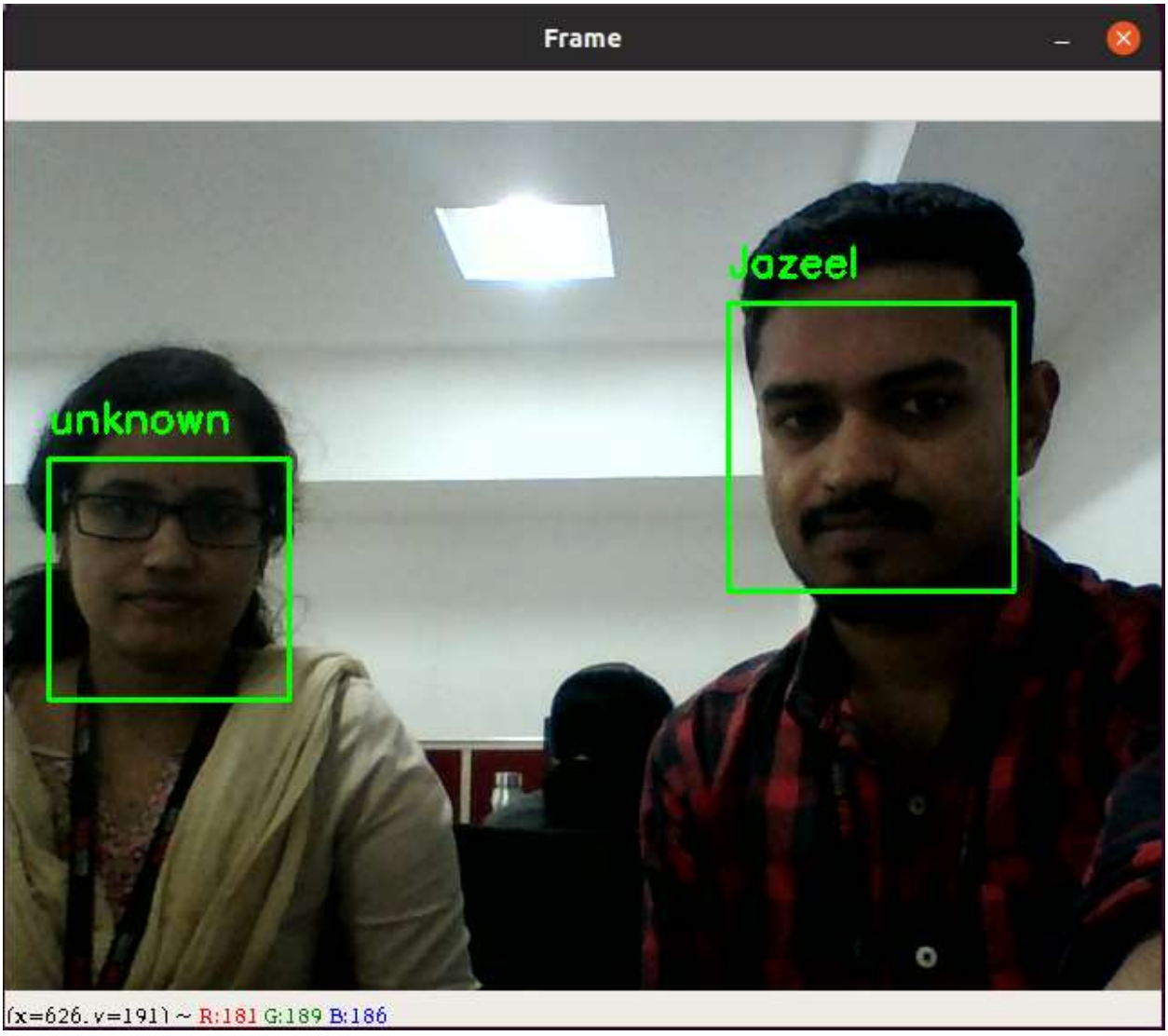
Output



a) Face Recognition



b) Spoofing detection



c) Unknown face detected

Conclusion

Almost all the biometric technologies require some voluntary action by the user, i.e., the user needs to place his hand on a hand-rest for fingerprinting or hand geometry detection and has to stand in a fixed position in front of a camera for iris or retina identification. However, face recognition can be done passively without any explicit action or participation on the part of the user since face images can be acquired from a distance by a camera. This is particularly beneficial for security and surveillance purposes. Furthermore, data acquisition in general is fraught with problems for other biometrics: techniques that rely on hands and fingers can be rendered useless if the epidermis tissue is damaged in some way (i.e., bruised or cracked). Hence this system found useful in attendance marking in the organization

Future Enhancements

System intend to improve face recognition effectiveness by using the interaction among our system, the users and the administrators. On the other hand, our system can be used in a completely new dimension of face recognition application, mobile based face recognition, which can be an aid for common people to know about any person being photographed by cell phone camera including proper authorization for accessing a centralized database. We can also add automatic door access system as an enhancement to this system to detect any unrecognized entry or unauthorized personal entry in to organization.