Smart Security using Artificial Intelligence

By

Name of the Team: dsp

DASARI PRADEEP KUMAR

DUDEKULA SAKINA

LAGISETTI MOUNIKA

1. Smart Security using Artificial Intelligence

1.1 Introduction

Security is a broad term, and in industry and government there are a myriad of “security” contexts on a variety of levels – from the individual to nation-wide. Artificial intelligence and machine learning technologies are being applied and developed across this spectrum.

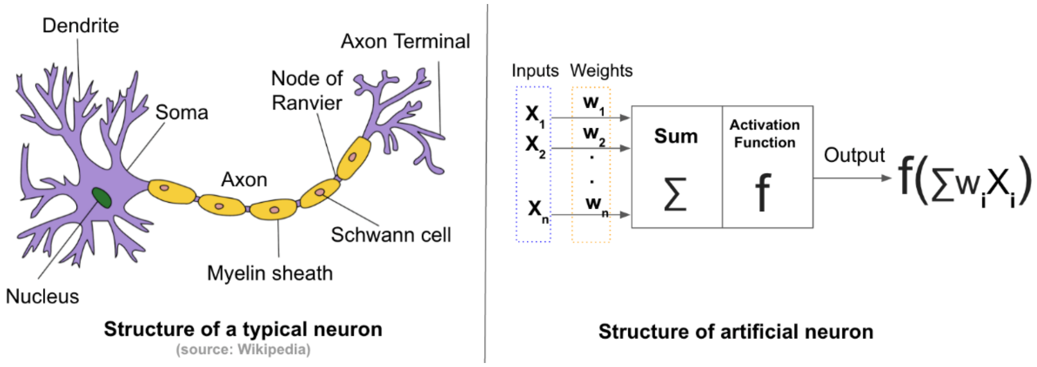
While many of these technologies have the potential and have greatly benefited society (helping reduce credit card fraud, for example), the evolving social contexts and applications of these technologies often leave more questions than answers – in terms of rules, regulations and moral judgments – in their wake. Artificial intelligence and security were – in many ways – made for each other, and the modern approaches of machine learning seem to be arriving just in time to fill in the gaps of previous rule-based data security systems.

Biometric based Security system is the mostly used one now a days and Face Identification or Authentication is another technique used in a very rare places and that too they’ll take a bit longer time to recognize. But, in this we’re going to implement the AI (Artificial Intelligence) to make it much accurate as well as much faster using CVV (Convolutional Neural Networks).

1.1.1 Convolutional Neural Networks

In deep learning, a convolutional neural network (CNN, or ConvNet) is a class of deep neural networks, most commonly applied to analyzing visual imagery.

CNNs are regularized versions of multilayer perceptron's. Multilayer perceptron's usually refer to fully connected networks, that is, each neuron in one layer is connected to all neurons in the next layer. The "fully-connectedness" of these networks make them prone to overfitting data. Typical ways of regularization include adding some form of magnitude measurement of weights to the loss function. However, CNNs take a different approach towards regularization: they take advantage of the hierarchical pattern in data and assemble more complex patterns using smaller and simpler patterns. Therefore, on the scale of connectedness and complexity, CNNs are on the lower extreme.



Structure of a typical neuron
(source: Wikipedia)

Structure of artificial neuron

Fig 1.1 Typical Neuron vs. Artificial Neuron

1.1.2 Keras

Keras prioritizes developer experience

- Keras is an API designed for human beings, not machines. Keras follows best practices for reducing cognitive load: it offers consistent & simple APIs, it minimizes the number of user actions required for common use cases, and it provides clear and actionable feedback upon user error.
- This makes Keras easy to learn and easy to use. As a Keras user, you are more productive, allowing you to try more ideas than your competition, faster -- which in turn helps you win machine learning competitions.
- This ease of use does not come at the cost of reduced flexibility: because Keras integrates with lower-level deep learning languages (in particular TensorFlow), it enables you to implement anything you could have built in the base language. In particular, as tf.keras, the Keras API integrates seamlessly with your TensorFlow workflows.

1.1.3 Tensorflow

TensorFlow is an open source software library for numerical computation using data-flow graphs. It was originally developed by the Google Brain Team within Google's Machine Intelligence research organization for machine learning and deep neural networks research, but the system is general enough to be applicable in a wide variety of other domains as well. It reached version 1.0 in February 2017, and has continued rapid development, with 21,000+ commits thus far, many from outside contributors. This article introduces TensorFlow, its open source community and ecosystem, and highlights some interesting TensorFlow open sourced models.

TensorFlow is cross-platform. It runs on nearly everything: GPUs and CPUs—including mobile and embedded platforms—and even tensor processing units (TPUs), which are specialized hardware to do tensor math on. They aren't widely available yet, but we have recently launched an alpha program.

1.2 Objective of Research

By making use of currently emerging Technologies like AI (Artificial Intelligence) and ML (Machine Learning) we thought to provide a high-end security product to an Organization so, that we can made it possible to control and limit unauthorized entry of the person(s) to the organization. By doing so we are/can be able to reduce or stop the important data loss and also misuse of the sensitive information. The same can be used in the places were a large number of people will move every day, and also in places were the attendance is required like Schools, Colleges, Offices, etc.,

1.3 Problem Statement

In our Daily life we're seeing the attendance-based system in many places from schools to a very large scaled office. In Schools the attendance system might be in the form of by calling their rolls or in rare cases it will be using Biometric based. In Offices and also in Colleges it is in the form of Biometric based system. All these systems are good enough just to take the attendance. But here it's consuming a lot of time to take the attendance. In this Project we're developing a **"Smart Security using Artificial Intelligence"** which will take the attendance just by looking up the candidate face(s) that too in seconds or in a fraction of seconds.

1.4 Industry Profile

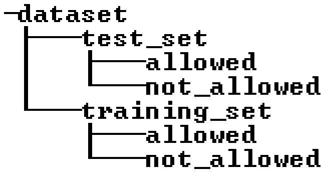
This kind of Applications can be implemented at Manufacturing Industries, Military, Army, Airforce, Schools, Colleges, Universities and also in research labs. Why because these are the major places where only authorized people are to be allowed and the others don't.

2. Review of Literature

The Dataset used to train this model is all pre collected images of the user(s). It can be made easy by passing the person under the camera for a while making him/her to express all his/her facial expressions. So that the model will gets trained on all possible cases of the person and can be able to recognize though the person is in any mood while he's passing under the camera.

3. Data Collection

The Collected data will be divided into Training Set and Test Set in the ratio of 4:1 so that the model will be able to train perfectly. For example, consider there were two kinds of people (let say 2 members) among them one is allowed and one is not. In such case we'll create two folders one is as "Train Set" and another one is as "Test Set". Then we'll make two more sub folders in them and name them as "allowed" and "not allowed" and then we'll place 80% of first person's photos in "Training Set" under "allowed" and 20% of the same person's photos in "Test Set" under the allowed folder. We'll apply same to the Second person too. The structure of the folder(s) will be like below.



```
─dataset
  ├───test_set
  │   ├───allowed
  │   └───not_allowed
  └───training_set
      ├───allowed
      └───not_allowed
```

4. Methodology

4.1 Data Modeling and Visualization

In this Application we collected all the data which is required for training and testing the model by using Webcam of the PC. We do collect a total of 1000 photos of two persons (500 + 500) and then we split them into 800 + 200 as training and test sets. Then Passed to the model for training as well as for testing.

The GUI will look like as below.

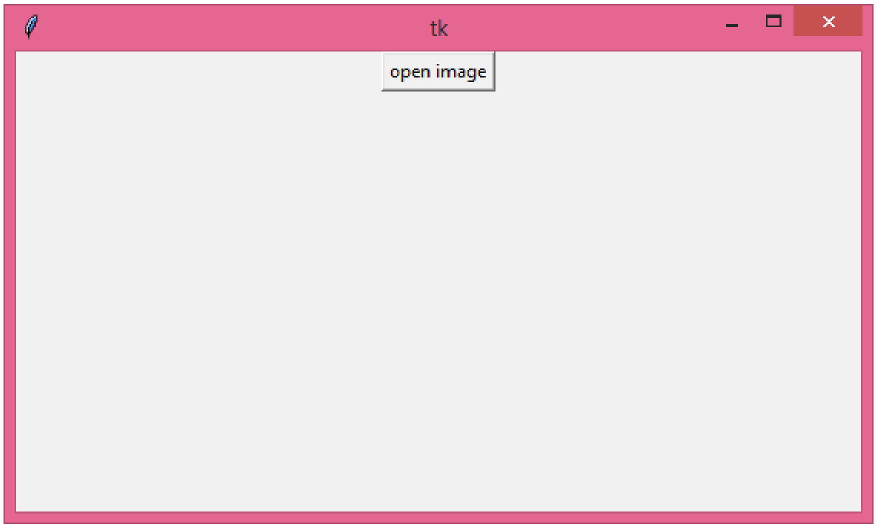
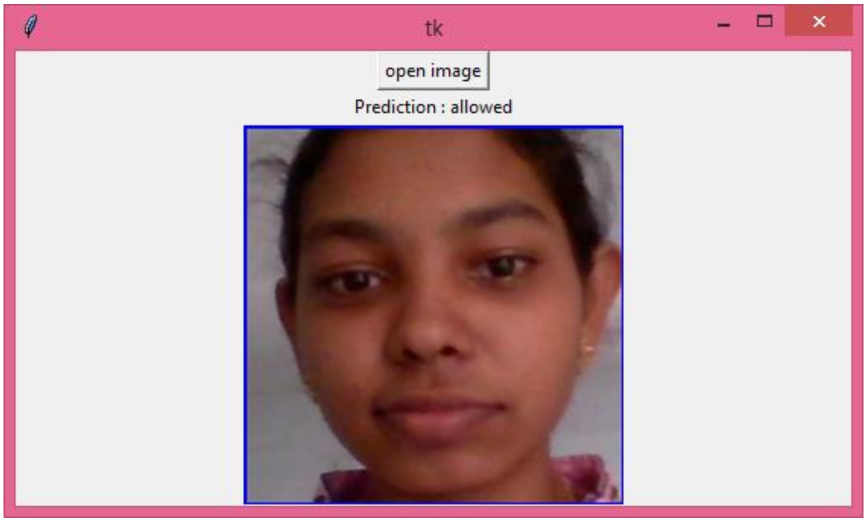
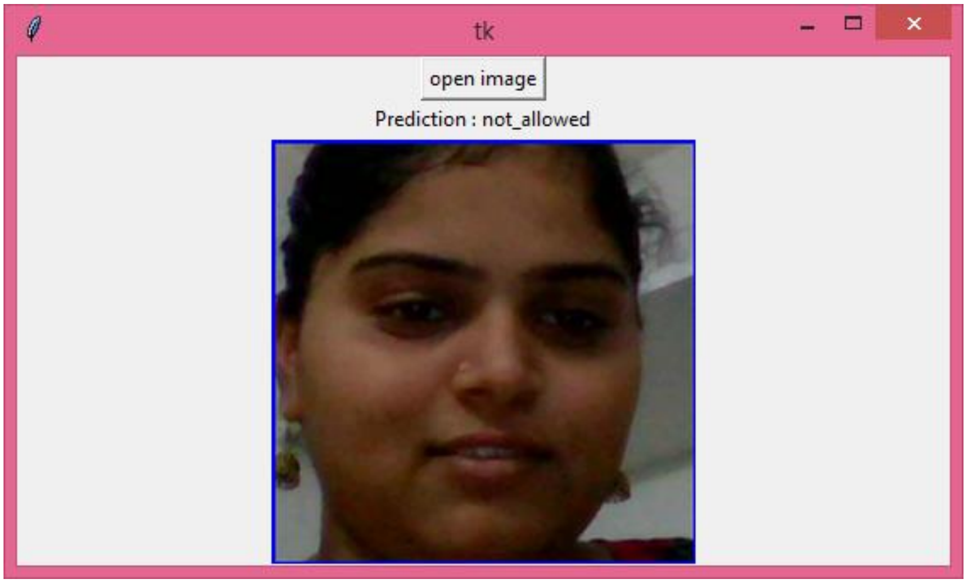


Fig 4.1 GUI before uploading the Picture.



Prediction : allowed

Fig 4.2 GUI After testing with the first person



Prediction : not_allowed

Fig 4.3 GUI After testing with the Second person

5. Findings and Suggestions

In this project we'd just created a prototype and it is to be implemented in a large scale with advanced cameras and also it needs a super computer and good Computational power for training the model and to save the results to a .h5 file. Once after saving the results there is no need of the supercomputer. It is be trained with the large number of samples of images.

6. Conclusion

Using Artificial Intelligence and a Few Libraries like Keras, Tensorflow and openCv we differentiated the people as allowed and not allowed and the same can be used in Industries, Organizations and Schools, etc., for security and safety reasons.