



Thesis Introduction

DIC MACHINE LEARNING



Facial Recognition and Face Mask Detection Using Machine Learning Techniques Learning Techniques. [Link](#)

Mira M. Boulos

Facial recognition has been widely used for security and other law enforcement Purposes. Facial recognition systems are biometric system that are used as a tool for identification processes. It identify individual identity by using their unique facial features. Biometric authentication systems identify individual using two set of features:

- 1) The physiological features uses the human features such as faces, irises, and fingerprints to identify a person.
- 2) The behavioral biometric uses features that result from action such as voice and handwritings.

This paper introduces a neural network system, which can be trained to identify people's facial features while half of their faces are covered by face masks. Using the Convolutional Neural Network(CNN), a large Face Mask detection dataset was used to train the model and the original much smaller Face Mask detector dataset was used to fine tune the train model. During the training and testing phase, the network structure and various parameters were adjusted to achieved the best accuracy of 97.1%.



Fawkes: Protecting Privacy against Unauthorized Deep Learning Models

Shawn Shan, Emily Wenger†, Jiayun Zhang, Huiying Li, Haitao Zheng, Ben Y. Zhao
[link](#)

The continual increase in the creation of powerful facial recognition systems is posing a real threat to personal privacy. As anyone can search the internet for data and train highly accurate facial recognition models of people without their knowledge.

This paper present Fawkes, a system that help individual to protect their images from unauthorized facial recognition models. Fawkes achieves this by helping users add small or invisible pixel-level changes called “cloaks” to their own photos before releasing them.

When used to train facial recognition models, these “cloaked” images produce functional models that consistently cause normal images of the user to be misidentified.

Fawkes provides 95+% protection against user recognition regardless of how trackers train their models. Even when clean, uncloaked images are “leaked” to the tracker and used for training, Fawkes can still maintain an 80+% protection success rate.



FaceNet: A Unified Embedding for Face Recognition and Clustering [link](#)

Florian Schroff Dmitry Kalenichenko James Philbin

In spite of the increasing advances in the field of face recognition, the present day approaches in implementing face verification and recognition efficiently is a serious challenge.

This paper presents a system called FaceNet that directly learns a mapping from face images to a compact Euclidean space where distances directly correspond to a measure of face similarity.

The method uses a deep convolutional network to train and the benefit of using this approach is it produces much greater efficiency. The system achieved an accuracy of 99.63% on the Labeled Faces in the Wild (LFW) dataset and 95.12% was achieved on the YouTube Faces dataset.

Deep Face Recognition

Omkar M. Parkhi, Andrea Vedaldi, Andrew Zisserman

[link](#)

either from a single photograph or from a set of faces tracked in a video, recent progress in the area face recognition has been due to two factors:

- (i) end to end learning for the task using a convolutional neural network (CNN), and
- (ii) the availability of very large scale training datasets.

This paper makes two contributions:

first, it shows how a very large scale dataset (2.6M images, over 2.6K people) can be assembled by a combination of automation and human in the loop, and discuss the trade off between data purity and time;

second, it traverse through the complexities of deep network training and face recognition to present methods and procedures to achieve comparable state of the art results on the standard LFW and YTF face benchmarks.



Learning Face Representation from Scratch

Dong Yi, Zhen Lei, Shengcai Liao and Stan Z. Li

[link](#)

Face recognition has been an active and vital topic among computer vision community for a long time and the performance of face recognition is becoming comparable to human.

Using private large scale training datasets, several groups achieve very high performance on LFW, i.e., 97% to 99%. While there are many open source implementations of CNN, none of large scale face dataset is publicly available. The current situation in the field of face recognition is that data is more important than algorithm.

To solve this problem, this paper proposes a semi - automatical way to collect face images from Internet and builds a large scale dataset containing about 10,000 subjects and 500,000 images, called CASIA WebFace. Based on the database, we use a 11-layer CNN to learn discriminative representation and obtain state-of-the art accuracy on LFW and YTF



Why this papers....

Sahr B. Sesay

Face recognition is playing an increasingly important role in modern life and has been widely used in residential security, face authentication (Wang et al. 2015), and criminal investigation.

Many security companies, government and businesses have adopted the use of facial recognition systems. This technology is becoming the main stream component of our every day lives from unlocking our smart phones to tagging our friends on Facebook.