Auto-unlocking your computer with a facial recognition system

(Proposed by Jianhua Li, Feb 20 2017)

1. Domain background

As the built in cameras becomes more and more common in cell phones and personal computers, images and videos are piling up. The desire to understand what is in these images and thus to apply this information to facilitate our daily life becomes more and more strong. Computer vision is an interdisciplinary field and provide a powerful solution in high-level image as well as videos understanding.

Face recognition, a form of computer vision, which uses the spatial geometry of distinguishing features of the face to identify or to authenticate a person. Software using webcam acquired images automatically log on an authorized user has been developed for many years by several companies. Computer access control system based on face recognition is also provided by three well-known computer manufacturers. Although it is convenient (hand-free), its security is one of the major concerns compared with other biometric recognition system. Nevertheless, it is still considered as a good supplement for current available solution.

2. Problem statement

For security reasons, we are required to lock our computer when we leave our desk. When we come back to our desk, we have to unlock it. There are multiple ways to do it, for example, one can type in the password through keyboard or use an external device to read identification information through smart ID card, but none of them are hand-free process. So it is kind of annoying to repeat these locking/unlocking steps manually. For this project, I propose to develop an auto-facial recognition system. This system uses the built in camera in the computer to capture the image of a person in front of it. To identify people, a 1:N authentication method is applied. Images of person authorized to use the computer are taken by myself. Images of unauthorized users are collected from online (like Faces94). Images are labeled with authorized (1) and unauthorized (0). A supervised learning model is generated with the machine learning algorithm such as support vector machine (SVM) or convolutional neural networks (CNN). The captured image will then be processed with OpenCV. Decision will be made based on the supervised learning model.

3. Datasets and inputs

Images collected from online Faces94 as well as taken by myself are presented as JPEG format. Images from online are taken from 153 individuals with 20 females and 133 males. Each individual have 20 images with minor variation in heard turn, title and slant. The resolution is 180 by 200 pixels. All images collected from online are labeled as unauthorized users. Images taken by myself are processed manually to the same format and resolution as those collected from online. Images prepared by myself (less than 100) are labeled as authorized users.

4. Solution statement

The relative small image dataset is preprocessed and data is extracted and converted into binary class matrices. An over-sampling strategy might apply to overcome the data unbalancing issue (3000 vs 100). Dataset is then divided into train, validation and test sets. Model will be learned by machine learning algorithms such as SVM and CNN. Image captured with the camera with be read and processed with OpenCV and further tested with learned model. Decision will be made based on the predicted result.

5. Benchmark model

Since this project deals with a sensitive security problem and the images pool is only limited to a specific user, one would expect the accuracy should close to hundred percent.

6. Evaluation metrics

The model is subjected cross validation. Since our dataset is a kind of unbalanced, final model will be evaluated with F1 score as well as confusion matrix. The system will be directly evaluated with the presence of a user in front of the computers. If an authorized user shown up in front of the computer, the computer will be automatically unlock so that the user does not need to manually unlock it. Otherwise, the computer will not do anything.

7. Project design

Step 1: Collect and preprocess data

Step 2: Generate and validate model

Step 3: Deploy model

Step 4: System testing

- Step 4.1: Capture live image
- Step 4.2: Process image

Step 4.3: Predict and classify image

Step 4.4: Make decision.

References:

1. Deep Learning Enables You to Hide Screen when Your Boss is approaching

2. Computer Vision Capstone Project

Figure. A diagram of facial recognition system