

C14 Open Source Automatic Facial Comparison Algorithms' Potential Application in Forensics

Angeliki Fydanaki, MFS*, Ohmstraat 8-III, Amsterdam 1098ST, NETHERLANDS; and Zeno J. Geradts, PhD*, Netherlands Forensic Institute, Laan van Ypenburg 6, Den Haag, SH 2497 GB, NETHERLANDS

After attending this presentation, attendees will understand several open source initiatives that exist for facial comparison as well as a test on forensic images.

This presentation will impact the forensic science community by introducing algorithms that are open source for facial comparison and discussing how they can be used in research.

The face is considered to be one of the main organs used in biometrics. It is a relatively stable part of the human body that has proven to be a great instrument in forensics. Over the past decade, the automatic facial analysis algorithms are at the center of the interest in the biometrics community. Recent facial comparison algorithms have illustrated significant growth regarding their performance; however, none were able to fill the gap between software and the significant high human accuracy. OpenFace is an algorithm that is trying to fulfill the aforementioned need. The center of this research is to determine the efficiency of the automatic OpenFace system as it relates to relevant forensic data. OpenFace is an open source toolkit based on the FaceNet algorithm, which has been created by Google[®]; however, it has been developed and shared as open source by Brandon Amos at Carnegie Mellon University. The main advantages of OpenFace are its online availability (which makes it a low-cost option), the limited need for human resources, and its reported performance on the Labeled Faces in the Wild (LFW)benchmark.

OpenFace requires specific products in order to operate, which are all open source as well; namely, OpenCV[®], Torch, GitHubTM, Docker, DlibTM, and a few libraries used in PythonTM. These products contribute to the three main tasks of OpenFace, which are verification, recognition, and clustering of faces on stable images and on real-time web videos. FaceNet, and hence OpenFace, are based on Euclidean embedding per image. Furthermore, they use the squared L2 distance in order to determine the face similarity of the query pair of faces. Then, by the use of one of the well-known techniques of K-means or agglomerative clustering, the recognition of the similar faces is achieved. Additionally, there is a triplet-based loss function used during training, which assures that the output of the algorithm is a compatible 128-D embedding. This sets a positive respective distance limitation. In general, this function minimizes the relevant distance when the same face is present on both query images and maximizes the relevant distance when different faces are present on the pair of query images. OpenFace could have multiple forensic applications. It could be used for facial recognition of suspects based on a query image and a reference; it could provide a connection of criminals by the use of images between multiple crime scenes; and it could be used with surveillance cameras in order to recognize specific individuals, as terrorists or a person reported as missing. Moreover, it could be used for the identification of corpses in mass disasters.

Based on the four OpenFace models and LFW benchmark, the verification of the reported results is achieved. The nn4.small2.v1 model outperforms the other three models in accuracy. For that reason, the further examination of nn4.small2.v1 model is selected. The experiments on OpenFace with the use of LFW-raw, LFW-deep funneled, SCface, and ForenFace datasets reveal that as the resolution of the input images is getting worse, the performance of nn4.small2.v1 OpenFace model is getting low. Moreover, the performance of OpenFace detector depends on the quality of the input images. This is due to the fact that it is unable to detect a face or align the input low-analysis

Copyright 2017 by the AAFS. Unless stated otherwise, noncommercial *photocopying* of editorial published in this periodical is permitted by AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by AAFS.



Digital & Multimedia Sciences - 2017

image. Furthermore, the runtime of OpenFace depends on the specifications of the machine in use and the quality of the image. This includes the fact that the detector processes images of low resolution more slowly. Hence, the intervention of the quality of the query images to the efficiency of OpenFace is forthright. Therefore, OpenFace proved inadequate in its current condition for forensic application. Notwithstanding, there are possible proposed improvements that are promising.

OpenFace, Open Source, Automated Facial Comparison

Copyright 2017 by the AAFS. Unless stated otherwise, noncommercial *photocopying* of editorial published in this periodical is permitted by AAFS. Permission to reprint, publish, or otherwise reproduce such material in any form other than photocopying must be obtained by AAFS.