B24 Why Automated Face Recognition Cannot Be Used to Eliminate Suspects

Richard Vorder Bruegge, PhD, FBI, OTD, Bldg 27958A, Pod E, Quantico, VA 22135*

After attending this presentation, attendees will understand that: (1) automatic Face Recognition (FR) is not designed to eliminate suspects, but to find potential matches; (2) even the best FR algorithms will have high false negative rates under a variety of conditions; and, (3) the variety of factors that lead to false negatives is so great, that using FR to eliminate suspects in the future is only likely to occur under the most restrictive of conditions.

This presentation will impact the forensic science community by making them aware of a key limitation of face recognition technology. It will also remove the presumption that just because a technology may be useful at including a subject in a pool of suspects, it cannot be assumed that it is equally capable of eliminating a subject.

Automated facial recognition (FR) has become an extremely useful tool for law enforcement and related government entities. For example, face recognition technology now allows numerous states to combat identity fraud by preventing criminals from obtaining driver's licenses under multiple identities. It was recently reported that New York State has had over 2,000 arrests for fraud since 2010 thanks to FR].[1] Likewise, law enforcement agencies have started to use FR to locate criminals who left their pictures behind while committing crimes.[2]

The success of these efforts results from over twenty years of steady improvement in the algorithms used to match faces. The most recent large-scale tests published by the National Institute of Standards and Technology (NIST) documented that the best face recognition algorithm tested had a false non-match rate of 0.3% when measured against a fixed false match rate of 0.1%.[3] This is a remarkable improvement, especially when one considers that the false non-match rate was close to 80% in 1993 when the NIST tests began![3]

The success of FR has led some in the criminal justice system to assume that it can be used equally well to exonerate individuals. This is not the case. While the NIST results provide strong evidence that FR can be used to identify potential matches, these tests were not designed to assess the degree to which FR can be used to eliminate subjects. Indeed, the point of this is made: "…a low score does not necessarily mean the images are of different persons. This arises because defective images produce low scores even in same-person comparisons. The term defective might mean low contrast, blurred, non-frontal pose, and exaggerated expression. "[3] Such "defects" are likely when comparing controlled images (e.g., mug shots) against uncontrolled images acquired from sources such as closed-circuit television (CCTV) systems. Likewise, other factors, such as aging and illumination changes, can also lead to low scores (i.e., false non-matches).[3]

In this study, a Government-OTS FR algorithm is used to demonstrate the variation in match scores for a number of same-person comparisons involving controlled and semi-controlled images. Although some high match scores are correctly returned, in many cases low scores are returned, with many falling below match scores generated in different-person comparisons. These results demonstrate the inability of current FR approaches to serve as a reliable means of eliminating suspects under all but the most highly controlled circumstances.

Given the variety of factors that can lead to low-match scores in same-person comparisons, it will be a challenge to acquire controlled datasets with sufficient sample size and variability to address all of these factors for all relevant populations. Instead, the best chance for developing FR algorithms to support the elimination of subjects will probably be limited to highly controlled applications.

References:

1. Choney, S., Facial recognition system nets 2,500 identity fraud arrests, NBC News Online report, March 5, 2013 (http://www.nbcnews.com/technology/facial-recognition-system-nets-2-500-identity-fraud-arrests-1C8692739 , accessed July 29, 2013).
2. Hausmann, J., NY Cops Use Face recognition on Facebook & Instagram to Nab Crooks, Heavy.Com report, March 29, 2013 (http://www.heavy.com/news/2013/03/police-face-recognition-facebook-instagram/ , accessed July 29, 2013).
3. Grother, P.J., Quinn, G.W. and Phillips, P.J., Report on the Evaluation of 2D Still-Image Face Recognition Algorithms**,** NIST Interagency Report 7709, August 24, 2011. (http://www.nist.gov/customcf/get_pdf.cfm?pub_id=905968 , accessed July 29, 2013).

 ** Presenting Author*

Face Recognition, Biometrics, False Negative

 ** Presenting Author*