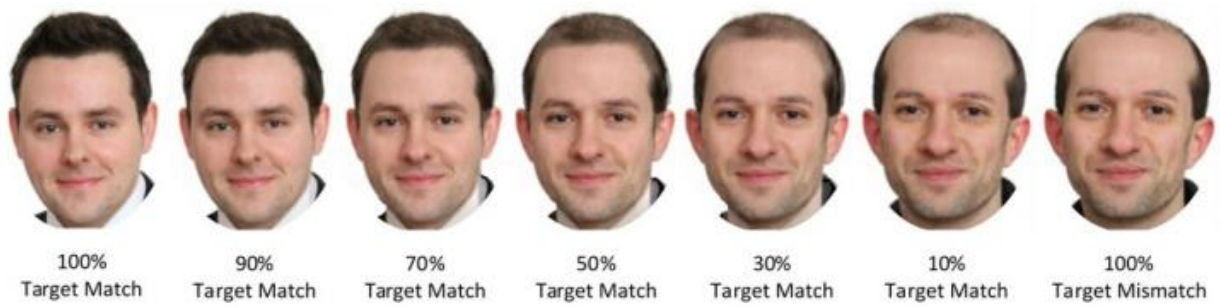
Humans and smartphones may fail frequently to detect face morph photos

March 22 2017



The stages of face morphing are shown. Credit: University of York

Researchers at the University of York have demonstrated that both humans and smartphones show a degree of error in distinguishing face morph photos from their 'real' faces on fraudulent identity cards.

Previous study at the University has shown that it is difficult to match a pair of unfamiliar faces - a photo of a person, against the real person - presenting significant issues for authorities to spot identity fraud.

Moving this research forward, the team investigated what the success rate would be like if two faces were morphed together to create a 'new' face. This involves taking two 'real' face photos and digitally blending them to make a new, but similar, face that both contributing faces can use as false ID.

Research, published in the journal *PLOS ONE*, has shown that both humans and smartphone software are frequently unable to distinguish face morph photos from the two faces contributing to the morph.

Professor Mike Burton, from the University of York's Department of Psychology, said: "We use photo ID all the time, not just at borders, and we know that people are not very accurate when matching the photo to the real face.

"In recent years we have seen more examples of photo IDs that have been created by morphing two faces together, which can be used as fraudulent ID by both parties. Our research is important in highlighting the potential security problem with this and quantifying the risk of this type of fraud being missed."

The authors of the present study examined the ability of both human viewers and smartphone face recognition software to identify a face morph as distinct from the two faces contributing to the morph. Human participants and smartphone software were asked to decide if a pair of faces matched. Sometimes, one of the pair was a morph photo and the other was one of the contributing faces.

The researchers found that initially, human viewers were unable to distinguish a 50/50 morph photo from its contributing photos 68 percent of the time. However, after simply briefing the viewers to look out for manipulated, 'fraudulent' images, the error rate dropped greatly to 21 percent.

The team also looked at smartphone software, which achieved similar results to briefed human viewers, with an error rate of 27 percent. These rates, however, are still significantly higher than error rates when comparing two photos of entirely different people.

Although, the participants in this study are unlikely to be as motivated or as skilled as a professional at spotting fraudulent photos, this study indicates that humans and smartphones may not naturally identify face morphs, a weakness that could be exploited by fraudsters.

Professor Burton said: "It is encouraging, however, that armed with the knowledge of morphed photo IDs, the risk of fraudulent activity being missed is significantly reduced.

"Raising awareness of this type of fraud and including it in training schemes for frontline staff can help overcome these issues, and with new technologies coming on line, it should be a challenge that can be tackled with some success."

Provided by University of York