Two fraudsters, one passport

August 1 2019

Credit: CC0 Public Domain

Computers are more accurate than humans at detecting digitally manipulated ID photos, which merge the images of two people, new research has found.

Face morphing is a method used by fraudsters in which two separate identity photographs are digitally merged to create a single image that sufficiently resembles both people. This image is then submitted as part of the application for a genuine passport or driving licence, and if accepted, potentially allows both people to use the same genuine identification document without arousing suspicion.

A new study by psychologists at the University of Lincoln asked participants in one experiment to decide whether an image showed the person standing in front of them. In this task, participants accepted the digitally created morphs around half of the time, while a basic computer model could correctly identify morphs over two thirds of time.

The research used high quality 'face morphs' over a series of four experiments which included screen-based image comparison tasks alongside a live task, designed to mimic a real-life border-control situation in which an agent would have to accept or reject a passport image based on its resemblance to the person in front of them.

Results showed that participants not only failed to spot 51 percent of these fraudulent images, but once they were provided with more information on face-morphing attacks, detection rates only rose to 64 percent. In another experiment, the researchers showed that training did not help participants to detect morphs presented onscreen, and detection rates remained around chance level. The results suggest that the morphs were accepted as legitimate ID photos often enough that they may be feasible as tools for committing fraud, especially in border control

situations where the final acceptance decision is often made by a human operator.

When similar images were put through a simple computer algorithm trained to differentiate between morphs and normal photos, 68 percent of the images were correctly identified as morph images, showing the programme to be significantly more accurate than human participants. The algorithm used was relatively basic as a demonstration, and recent software being developed by computer scientists is far more sophisticated and shows even greater levels of success.

Lead researcher Dr. Robin Kramer from the University of Lincoln's School of Psychology said: "The advancements and availability of high quality image editing software has made these kinds of 'face morphing attacks' more sophisticated and the images harder to detect.

"Our results show that morph detection is highly error-prone and the level at which these images were accepted represents a significant concern for security agencies. Training did not provide a useful solution to this problem.

"Our research could be significant for security agencies and suggests that the use of computer algorithms may be a better method for minimising how often these kinds of morphing attacks slip through the net."

More information: Robin S. S. Kramer et al, Face morphing attacks: Investigating detection with humans and computers, *Cognitive Research: Principles and Implications* (2019). DOI: 10.1186/s41235-019-0181-4

Provided by University of Lincoln