PLOS Science Wednesday: Hi reddit, my name is David and my PLOS ONE study shows untrained humans and computers make similar errors when confirming identification by facial recognition – Ask Me Anything!

PLOSScienceWednesday [1] and r/Science AMAs[1]

[1]Affiliation not available

April 17, 2023

Abstract

Hi Reddit, My name is Dr. David Robertson and I am Teaching & Research Fellow at the School of Psychological Sciences & Health, University of Strathclyde, Glasgow (UK). My research focuses on applied face recognition and the use of this biometric in policing and security contexts. I recently published a study (Robertson DJ, Kramer RSS, Burton AM (2017)) titled Fraudulent ID using face morphs: Experiments on human and automatic recognition in PLOS ONE. Across three experiments we assessed the extent to which human operators and a smartphone algorithm accepted face morphs as a genuine match to a target face. Face morphs do represent a route to identity fraud in humans and machine recognition systems, human detection of these images can be improved through awareness training. I will be answering your questions at 1pm ET. Ask me Anything! Don't forget to follow me on Twitter @UOSPsychology York FaceVar Lab website here.

the WINNOWER

REDDIT

PLOS Science Wednesday: Hi reddit, my name is David and my PLOS ONE study shows untrained humans and computers make similar errors when confirming identification by facial recognition – Ask Me Anything!

PLOSSCIENCEWEDNESDAY R/SCIENCE

Hi Reddit,
My name is Dr. David Robertson and I am Teaching & Research Fellow at the School of Psychological Sciences & Health, University of Strathclyde, Glasgow (UK).
My research focuses on applied face recognition and the use of this biometric in policing and security contexts.
I recently published a study (Robertson DJ, Kramer RSS, Burton AM (2017)) titledFraudulent ID using face morphs: Experiments on human and automatic recognition in PLOS ONE.
Across three experiments we assessed the extent to which human operators and a smartphone algorithm accepted face morphs as a genuine match to a target face. Face morphs do represent a route to identity fraud in humans and machine recognition systems, human detection of these images can be improved through awareness training.
I will be answering your questions at 1pm ET. Ask me Anything!
Don't forget to follow me on Twitter @UOSPsychology
York FaceVar Lab website here.

CORRESPONDENCE:

DATE RECEIVED:
May 18, 2017

DOI:
10.15200/winn.149502.25471

ARCHIVED:
May 17, 2017

CITATION:
PLOSScienceWednesday , r/Science , PLOS Science Wednesday: Hi reddit, my name is David and my PLOS ONE study shows untrained humans and computers make similar errors when confirming identification by facial recognition – Ask Me Anything!, *The Winnower* 4:e149502.25471 , 2017 , DOI: 10.15200/winn.149502.25471

Thanks for being here today! Can you explain more about the nature of how the face morphs tricked people? There was a popular post on reddit suggesting computers struggled to differentiate between a Chihuahua and a muffin, where the first comment showed a similar result for dogs and fried chicken. While the similarity is obvious, humans wouldn't struggle to differentiate between these images. Can you tell us a bit more about the cases where both the algorithm and humans failed to correctly identify the face morph? Can you share some example pictures? Can you also explain this comment a bit more "Face morphs do represent a route to identity fraud in humans and machine recognition systems"- eg what is a scenario where face morphs and algorithmic identification would help identify identity fraud?

p1percub

Hi p1percub, thanks for your question! In each of the three experiments, the task is essentially a 1(face photo)-1(face photo) matching task. In Experiment 1, human participants were not informed about the use of face morph stimuli in the experiment. They were simply shown a face photo on of a person on the left of the screen, and a passport photo on the right side of the screen. They had to decide whether the images showed the same person (match) or two different people (mismatch). The general term for this is UNFAMILIAR face recognition (we do not know the people whose photos we are presented with), and in having no awareness of the morphs, this is likely to mirror the current context in which morph fraud is unlikely to be widely known, be part of fraud prevention literature or anti-fraud training

packages. This type of unfamiliar 1-1 face matching task is common in everyday situations. For example, at border control we ask a border official to decide whether a passport photo (which could be up to 10 years old) matches the face of an unfamiliar traveller standing in front of them. An error here results in a fraudster entering the country. In another example, police and law enforcement officials may be required to match a poor quality facial image of a suspect from CCTV to a person in a database of large custody images. An error in this situation would lead to the investigation being taken in the wrong direction (at best), and a wrongful conviction (at worst). In retail, we ask those who look underage to produce a photo ID card to prove that they are old enough to buy age restricted good such as cigarettes and alcohol. Again, the retailer is being asked to try and match an unfamiliar person's face to the photo-ID image. Now research from Professor Mike Burton, Dr. Rob Jenkins, myself, and others have shown that while we can effortlessly recognise new instances of familiar people (friends, family, colleagues) even with high levels of variation in their appearance (ageing, lighting, changes in hairstyle for example), when it comes to recognising a new instances of an UNFAMILIAR person, this is a task that is difficult and highly prone to error. Because we have no knowledge of the extent to which an unfamiliar person's face can vary, we can often accept a photo of an entirely different person as a match to the target face (error rates can reach levels of 30% here). Despite these well-established findings unfamiliar face recognition is still used in the situations mentioned above. To ID commit ID fraud, a fraudster procures an image and identity details of someone that looks like them (if the fraud is to be successful). However, what this paper states is that, with the advance of image manipulation software, the fraudster could now take an image that looks less like them (providing more opportunities for fraud) and morph or 'blend' their face and the victims face together. By doing so, the image could contain 50% of the fraudsters face and 50% of the victim's. In this way, the fraudster now has an image that could be used to fool passport renewal officials and border officials. Example stimuli can be seen in the paper: http://journals.plos.org/plosone/article?id=10.1371/journal.pone.0173319

Do you think the reason why people and computers make similar errors comes down to the fact that people made the computers or do you think there's another reason?

saevuswinds

This is a really good question, I think the answer is that both humans and machines struggle with the problem of within-person variation in appearance when we are dealing with people who are unfamiliar to us.

Are humans not "trained" from birth at this task?

elrugmunchero

Human face recognition abilities are an individual difference. People who are really good at face recognition (I never forget a face) are known as Super-recognisers, while those that, through brain damage for example, have trouble recognising familiar members are known to have prosopagnosia. And within those two extremes are most of the population. Much like some people can't sing (like me!), some are excellent (like Fleetwood Mac) and others lie somewhere in between.

I noticed that your photo examples for your study were all white and male. There has been some interesting and important criticism that facial recognition software is often poor at recognizing black people in part because the examples used for the algorithms are largely non-black (see work done by Joy Buolamwini.)

Will you repeat this experiment using people from non-white backgrounds and who aren't male? How

do you think that might impact the results?

Also, what were the demographic backgrounds of the people in this experiment? Do you think the issue of facial recognition software being poor at recognizing black faces due to poor exposure to varied face types would also be an issue for humans (i.e. your participants might be poor at detecting difference between people with face types they have little exposure to)?

firedrops

The stimuli used in this experiment came from the Glasgow Face Matching Test (Burton et al, 2010), a well established test of unfamiliare face recognition. Faces were all Caucasian, the age range was ~18-65 if I recall correctly. See posts above for information on the other race effect in the face recognition literature.

As a computer scientist I am curious, what are you using for the image processing and recognition? Have you used Convolutional Neural Networks and Recurrent Neural Networks to study this behavior? Any common Deep Learning processes used?

GamerFan2012

Hi GamerFan, have a look at the publications section of our website,www.facevar.com, there is some recent work on this, I think, from our computational strand of researchers.

I find that discussions of face recognition often quickly go somewhere rather dystopian. Has this been your experience, and does it frustrate you? Or do you think these area valid concerns?

recentfish

Hi recentfish, I think, and have a look at our work at facevar.com, that there is a very real issue with using face recognition in policing and security contexts - the problem of within-person variability in appearance for unfamiliar people is the key stumbling block here. With emerging technologies, finger prints or iris scans may be the way forward (or even physiological patters such as individual heart rhythms, I've seen some work on that too).

do you like taquitos? my wife says they're gross but i like them, back me up man!

Trumpeachment

Dude, I'm Scottish, I like haggis and deep fried Mars Bars (google it!)

Hello David,

My question is that I'm wondering if there's any defense against prosthetics being used to provide a false match?

StellarValkyrie

Hi StellarValkyrie, great question, we know from research (for example from Michael Tarr's lab) that disguise lowers the unfamiliar face recognition rate further. At present, I haven't yet seen any work which has shown a way to overcome that. One promising avenue may be with super-face-recognisers (see paper link below), who show above average face recognition abilities.

http://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0150036

Hi

Thanks for doing this. What's the accuracy of facial recognition today? And how easily can it be tricked?

FreedomKayak

Hi FreedomKayak,

Great question, have a look at my posts above for more detailed information on this, but the general answer is that while we may be expert face recognisers when it comes to recognising new instances of people we are familiar with, this ability does not generalise to unfamiliar face recognition. Error rates for accepting a photo of an entirely different person as a match to an unfamiliar person's face can reach as high as 30%. In relation to the contexts in which we use facial biometrics, this is a non-trivial level of error, some more information in the links below.

Metropolitan Police Super-recognisers: http://journals.plos.org/plosone/article?id=10.1371%2Fjournal.pone.0150036

Face Averages Improve Machine Recognition: https://pure.strath.ac.uk/portal/en/publications/could-super-recognisers-be-the-latest-weapon-in-the-war-on-terror(1b208228-590b-41e4-9a43-956349525046).html

Unfamiliar Face Recognition Research Review: https://drive.google.com/file/d/0B3xE1VVFqo_LOUl2UjlnYnpuam8/view

www.facevar.com