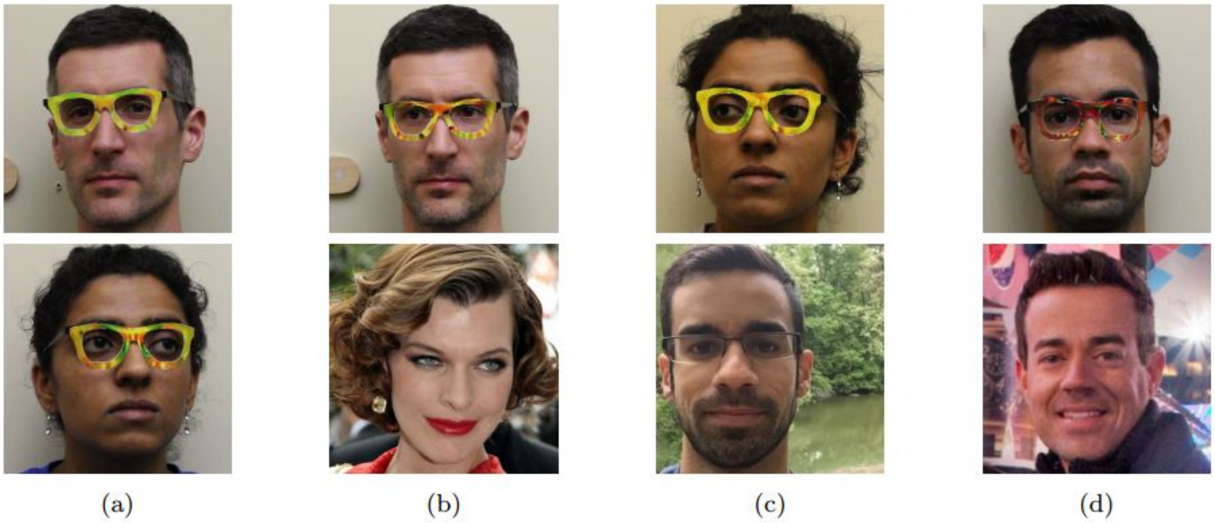
Who are you looking at? Glasses fool face recognition software

November 7 2016, by Nancy Owano



Examples of successful impersonation and dodging attacks. Fig. (a) shows SA (top) and SB (bottom) dodging against DNNB. Fig. (b)–(d) show impersonations. Impersonators carrying out the attack are shown in the top row and corresponding impersonation targets in the bottom row. Fig. (b) shows SA impersonating Milla Jovovich (by Georges Biard / CC BY-SA / cropped from https://goo.gl/GlsWlC); (c) SB impersonating SC ; and (d) SC impersonating Carson Daly (by Anthony Quintano / CC BY / cropped from goo.gl/VfnDct). Credit: Mahmood Sharif et al.

(Tech Xplore)—Can snazzy specs be a secret weapon for someone avoiding surveillance? A team of researchers used a change in physical appearance to confuse face recognition software.

Eyewear printed with a wild pattern did the trick to avoid facial identification. Timothy Revell said in *New Scientist* that the team "fooled face recognition algorithms using the oldest trick in the book: a pair of fake glasses."

The researchers presented their paper at a 2016 conference on Computer and Communications Security. The title is "Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition," by authors Mahmood Sharif, Sruti Bhagavatula, Lujo Bauer (the three are from Carnegie Mellon) and Michael Reiter, University of North Carolina at Chapel Hill.

The tests they used had two impressive gains, of not only fooling facial recognition tech but also appearing to look like other people. In analyzing differences between one face and the other which they wanted it to be mistaken for, the team was able to work out how to confuse the software.

"By printing bespoke patterns onto the front of the frames, they enabled wearers not only to obscure their identity but to impersonate people who look completely different, at least in the eyes of the algorithm."

The team, in discussing printing a pair of eyeglass frames in their paper, said, "When worn by the attacker whose image is supplied to a state-of-the-art face-recognition algorithm, the eyeglasses allow her to evade being recognized or to impersonate another individual."

Revell discussed these impersonation feats further. "A white male researcher wearing the glasses was able to pass for American actress Milla Jovovich while a South-Asian female colleague was digitally disguised as a Middle-Eastern male." Revell said that they tricked commercially available face recognition software with a success rate of about 90%.

So just how did the team fool the recognition technology? *New Scientist* said the glasses were used to exploit the recognition system's neural networks.

"The systems often focus on things like the colour of different pixels and slowly piece together a best guess of who's in the shot by comparing it to other, similar images. If just a small area of the face has been changed, it can completely mess with the attempted recognition – which is why the computer system can confuse two people who in fact look very different," said Revell.

New Scientist quoted one of the authors, Sharif. "We're starting to find that neural networks don't always have the flexibility that we once thought they had," and just "a few small targeted changes can have a large overall effect in tricking the software."

Alex Hern, technology reporter for the *Guardian*, reported on their system where, using a normal photo printer, the patterns printed over the eyeglass frames served to do the job to manipulate an image.

But initially the researchers "struck gold," Hern said, in realizing that a large-ish pair of glasses could act to change pixels in a photo.

The frames may just look like a colorful design, said Revell, but "The frames essentially overlay the face with pixels that perturb the software's calculations in just the right way that it misidentifies the person as another specified face in its database."

Discussing their work, the authors stated that "In this paper, we demonstrated techniques for generating accessories in the form of eyeglass frames that, when printed and worn, can effectively fool state-of-the-art face recognition systems."

Mahmood Sharif said in *New Scientist*, "With some refinement, our glasses would just look like someone had frames with a normal tortoiseshell pattern."

More information: Research paper: Accessorize to a Crime: Real and Stealthy Attacks on State-of-the-Art Face Recognition: www.cs.cmu.edu/~sbhagava/papers/face-rec-ccs16.pdf

Citation: Who are you looking at? Glasses fool face recognition software (2016, November 7) retrieved 2 May 2024 from https://techxplore.com/news/2016-11-glasses-recognition-software.html