3311101694 · 研究生英语国际学术交流

胡玉斌 / 202111054

pre 汇报稿

December 5, 2021

p1

Few biometric technologies are sparking our imagination quite like face recognition. Equally, its arrival has prompted profound concerns and surprising reactions this year.

But more about that later.

p2

It's a joke, of course, but we can't help but wonder: can someone really imitate my face? Or, will some system that can recognize my face be hacked? The answer is yes.

Before introducing the attack, let's understand how facial recognition works.

p3

Facial recognition is the process of identifying or verifying the identity of a person using their face. It captures, analyzes, and compares patterns based on the person's facial details.

- The face detection process is an essential step in detecting and locating human faces in images and videos.
- The face capture process transforms analog information (a face) into a set of digital information (data or vectors) based on the person's facial features.
- The face match process verifies if two faces belong to the same person.

Here are three photos corresponding to these three steps.

p4

Back to our original question: can someone really imitate my face? Or， Can face recognition be fooled?

- Grigory Bakunov developed an algorithm that creates special makeup to fool the software. It can escape proper face detection and confuse face detection devices.
- Berlin artist Adam is now working on clothing featuring patterns to prevent detection. The hyperface camouflage includes patterns in fabric, such as eyes and mouths, to fool the face recognition system.
- Researchers from a German company revealed a hack that allowed them to bypass the facial authentication of Windows 10 Hello by printing a facial image in infrared.

And their attacks continue and will get stronger.

This will create an unprecedented challenge for society.