Adversarial attacks are striking not only for AI (machine learning) but also for humans and a variety of sensors

Yoshiyasu Takefuji

Matthew Hutson mentioned that adversarial attacks easily fool artificial intelligences (1). Adversarial attacks can also fool us easily. We, human-beings are inherently confused with images. Especially Escher created a variety of simulacra/contradictory images. A simulacrum is a representation or imitation of a person or thing. Provided an image, we mistakenly recognize someone or something, or are simply confused. See simulacra site (2). According to Wikipedia, the term **illusory motion**, also known as **motion illusion**, is an optical illusion in which a static image appears to be moving due to the cognitive effects of interacting color contrasts and shape position. We are always vulnerable against such illusions. AI (machine learning) system is also confused with images (3). Adversarial attacks are striking not only for humans but also for AI. A variety of sensors are vulnerable against adversarial attacks. Latest autonomous cars can be fooled by spoofing GPS (Global Positioning System) sensors, LiDAR (Light Detection and Ranging) sensors, and cameras (4).

References:

1. Matthew Hutson, Hackers easily fool artificial intelligences, Science 20 Jul 2018: Vol. 361, Issue 6399, pp. 215
2. http://www.ohmidog.com/tag/simulacra/
3. Y. Takefuji, TASC monthly no.512
http://www.tasc.or.jp/educate/monthly/2018/index.html
4. Y. Takefuji, http://science.sciencemag.org/content/361/6397/36/tab-e-letters