禪

حمله تصویری به سامانههای هوشمند پزشکی

کمک ماشینها به بهتر دیدن ما، از نتایج مهم استفاده از روشهای پردازش تصویر و یادگیری ماشین در دنیای جدید است. تقویت آنچه میبینیم کمک بزرگی در زندگی روزمره ما خواهد بود. بهطور مثال ماشینهای بینایی که در پزشکی استفاده میشوند، هنوز قابلاعتماد نیستند و بهراحتی فریب میخورند. آثار چنین ایرادی هم میتواند به قیمت جان انسانها تمام شود و در خوشبینانهترین حالت، ضرر مالی به آنها بزند

بهسادگی میتوان با روشی موسوم به حمله تخاصمی (Adversarial Attacks) یک سامانه هوشمند تجزیهوتحلیل تصاویر پزشکی را فریب داد. در این حمله مهاجمان با ایجاد تغییراتی اندک و البته حسابشده در دادههای تصویری، بدون اینکه توجه کاربر جلب شود، الگوریتم را به اشتباه میاندازند. مدتی پیش گروهی از محققان دانشکده پزشکی هاروارد و دانشگاه اِمآیتی با تغییر دادن چند پیکسل از تصاویر پزشکی موفق به فریب دادن سامانه یادگیری ماشینی شدند که بر اساس تصاویر پزشکی، بیماری افراد را تشخیص میداد. حالا همین گروه از محققان با همکاری یکی از کارشناسان دانشکده حقوق هاروارد پیشنهادهایی در زمینه رویارویی با چنین حملاتی مطرح کردهاند. آنها معتقدند، اگرچه هنوز زمان داریم اما باید برای دفاع آماده باشیم.

Fundoscopy
Chest X-Ray
Dermoscopy
Absent/mild DR
Moderate/Severe DR
Normal
Pneumothorax
Nevus
Melanoma
Clean
PGD
Nat. Patch
Adv. Patch
0.0%
100.0%
0.2%
99.%
0.0%
100.0%
100.0%
0.0%
100.0%
0.0%
100.0%
0.0%
0.01%
99.9%
0.3%
96.7 %
69.7%
54.2%
98.3%
35.0%
100.0%
0.1%
100.0%
0.0%

.[illegible]

[illegible] [illegible] [illegible] [

[illegible] ground zero [illegible].

[illegible]:
[illegible]
[illegible]:
[illegible]
[illegible]:
21:55 - 21/03/1398
[illegible]:
[illegible] - [illegible] - [illegible] - Adversarial Attacks - [illegible] - [illegible]

[illegible]
[illegible]: https://www.shabakeh-mag.com/information-feature/15418/%D8%AD%D9%85%D9%84%D9%87-%D8%AA%D8%B5%D9%88%DB%8C%D8%B1%DB%8C-%D8%A8%D9%87-%D8%B3%D8%A7%D9%85%D8%A7%D9%86%D9%87%E2%80%8C%D9%87%D8%A7%DB%8C-%D9%87%D9%88%D8%B4%D9%85%D9%86%D8%AF-%D9%BE%D8%B2%D8%B4%DA%A9%DB%8C