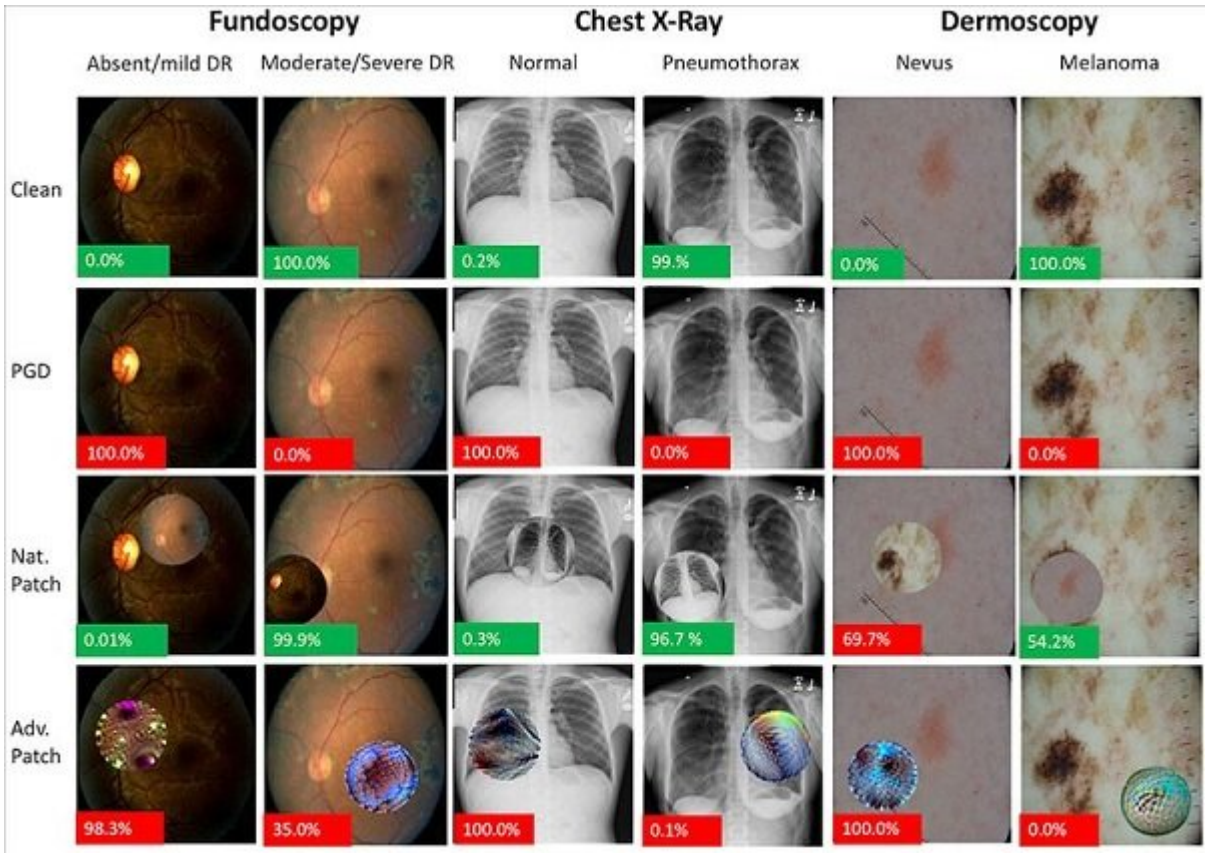
حمله تصویری به سامانه‌های هوشمند پزشکی

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.



دلایل متنوعی برای اجرای چنین حمله‌هایی وجود دارد. برخی از پزشکان و بیمه‌گذاران انگیزه‌های زیادی برای اجرای حمله‌های تخاصمی به سامانه‌های هوشمند پزشکی دارند و مهم‌تر از همه این‌که پیاده کردن چنین حمله‌هایی به نسبت ساده است. به‌طور مثال، کافی است در زمان گرفتن عکس از یک خال روی پوست، کمی دوربین را بچرخانید تا الگوریتم تشخیص پزشکی به اشتباه افتاده و این خال را نشانه یک سرطان بدخیم پوست تشخیص دهد. بااین‌حال، به عقیده این محققان اگرچه امکان چنین حملاتی وجود دارد اما هنوز جنبه عملی نیافته‌اند. آن‌ها هشدار می‌دهند که باید تا پیش از فراگیر شدن چنین حملاتی راهی برای مقابله با آن‌ها یافت.

مطلب پیشنهادی

ماشین‌های بینایی که فریب نمی‌خورند
فریب دادن شبکه‌های عصبی

جاناتان زیتراین، از دانشکده حقوق دانشگاه هاروارد و نویسنده کتاب «آینده اینترنت و چگونگی توقف آن» بر اساس نتایج پژوهش این محققان چنین می‌گوید: «حدود بیست سال پیش را به خاطر آوردم، زمانی‌که آسیب‌پذیری در حوزه امنیت سایبری به‌وضوح دیده می‌شد، ولی اقدامات عملی چندانی انجام نشد.» او معتقد است نباید تمرکز خود را بر پیش‌بینی هر چیز بدی بگذاریم که ممکن است یک فناوری جدید با خود به همراه بیاورد. بلکه کافی است زمانی‌که با آن‌ها مواجه شدیم، اطلاع‌رسانی کنیم و راهی برای مقابله با آن بیابیم. به عقیده او، پیش‌بینی و یافتن راهی برای پیشگیری از انواع حمله‌ها ممکن به یک سامانه هوشمند پزشکی، تنها باعث کند شدن روند توسعه ابزارهای مفیدی خواهد شد که می‌توانند به جوامع مختلف کمک کنند نظیر سامانه‌های هوشمند پزشکی که با استفاده از آن‌ها می‌توان به ساکنان مناطق محرومی که دسترسی به پزشک متخصص ندارند، کمک کرد. او استفاده از روش‌های کارآمد موجود نظیر آزمودن آسیب‌پذیری‌های سامانه‌ها پیش از به‌کارگیری آن‌ها یا رمزگذاری تصاویر به‌منظور شناسایی دستکاری احتمالی آینده را بهترین روش برای آمادگی در برابر چنین حمله‌هایی می‌داند و تنها در این صورت است که در زمان

بروز حمله‌ها، استفاده از روش‌های دفاعی مؤثر خواهند بود. از سوی دیگر، به عقیده زیتراین می‌توان گام‌های تکمیلی دیگری را برداشت، نظیر بررسی مداوم عملکرد سامانه توسط کسانی‌که آن را آموزش داده‌اند تا در این صورت نتیجه‌گیری‌های نامربوط و عجیب احتمالی شناسایی شوند. اگر چه این نوع حمله‌ها بیشتر در کنفرانس‌ها ارائه شده‌اند و در محصولات موجود در بازار به‌ندرت دیده می‌شوند، اما محققان بر این باورند، حوزه سلامت می‌تواند یک ground zero برای حمله‌های تخاصمی حقیقی باشد.

تاریخ انتشار:
21 خرداد 1398

نشانی منبع:
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