

# فناوری و رسانه

در باب ماشین های هوش دزد

## نگرانی از مداخله هوش مصنوعی در هویت افراد

ونوس بهنود

دبیر تحریریه

جوانسازی واقعیت ببخشید. برای ارزیابی دقت مدل خود، محققان یک مطالعه انجام دادند که در آن از داوطلبان خواسته شد تا تصاویر تولید شده با عکس های واقعی همان افراد را مرتبط کنند. نتایج نشان داد که تا ۴۴ درصد، در عملکرد برتری داشته است. جالب است که محققان متوجه شدند ترکیب مجموعه آموزش بر عملکرد مدل تأثیر داشته است. داشتن تصاویر از دسته های سنی متنوع منجر به نمایندگی مؤثر از گروه سنی های مختلف می شود. با این حال، اگر مجموعه آموزش اصلاً از تصاویر سالخورده تشکیل شود، تولید تصاویری از سنین متناقض مانند کودکان چالشی خواهد بود. محققان همچنین مشاهده کردند که مدل، در تبدیل تصاویر آموزشی به گروه های سنی بزرگتر برای مردان نسبت به زنان بهتر عمل می کند، احتمالاً به دلیل شامل شدن آرایش در تصاویر آموزشی.

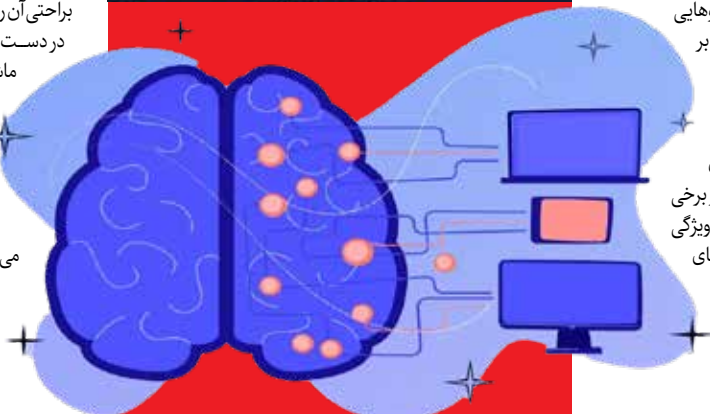
### چه کسی می تواند به اقدام هوش مصنوعی پی ببرد؟

با وجود اینکه هوش مصنوعی از مرحله آرایش و تغییر لباس به تغییر نژاد، سن و حتی هویت افراد توانمند شده است اما همچنان دست انسان این ماشین را قدرتمند ساخته است. در هوش مصنوعی سناریوهای مختلفی برای تشکیل الگوریتم در اختیار سیستم قرار می گیرد و پس از آن دیگر سیستم به دستورالعمل خاصی نیاز ندارد و می تواند بر اساس الگوریتم های خود عمل کند. اما بهترین توانایی هوش مصنوعی این است که می تواند اشتباهات مدل های آموزشی کمک بگیرد، به عبارتی هوش مصنوعی می تواند اشتباهات خود را اصلاح کند. هوش مصنوعی اکنون در فناوری تشخیص چهره ادغام شده و می تواند بدون نظارت دائمی انسان، یک فرایند تأیید هویت بدون وقفه را انجام دهد. چهره فرد از طریق شناسایی چهره با هوش مصنوعی اسکن شده و با عکس موجود در سند هویت فرد تطبیق داده می شود. آزمایش تشخیص زنده بودن نهایی، ویژگی های عضلات صورت کاربر را تجزیه و تحلیل می کند. همچنین هوش مصنوعی برای تشخیص چهره از روی عکس و تصویر است یا فرد در لحظه در آن مکان حضور دارد، اگر تلاشی برای جعل صورت بگیرد سیستم آن را تشخیص داده و تأیید ناموفق خواهد بود. درک عمق سه بعدی شامل تجزیه و تحلیل عمق چهره از طریق بافت پوست و نقاط صورت انجام می شود. همه اینها در نهایت در کنار هم موجب این می شود که اگر یک کلاهبردار برای جعل هویت شخص دیگری اقدام کند، تشخیص چهره با استفاده از هوش مصنوعی برای آن را تشخیص می دهد. بر این اساس زمانی که کنترل همه چیز در دست هوش مصنوعی است آیا نگرانی دانشمندان از قدرت گرفتن ماشین هایی که حتی هویت ما را می دزدند به جا نیست؟

بسیاری از اتفاقات در مدت زمان اندکی در حال رقم خوردن است و بحران هویت یکی از موضوعات کلیدی خواهد بود که بشریت بزودی گرفتار آن می شود. این در حالی است که روز به روز نیز به کاربران هوش مصنوعی که اطلاعات و داده های خود را در دهان این ماشین می ریزند و آن را نقد می کنند، اضافه می شود.

می دهد. برنامه هوش مصنوعی چهره SwapFace یکی از ابزارهای موجود در این زمینه است. محققان مدرسه مهندسی تاندون دانشگاه NYU یک تکنیک هوش مصنوعی جدید توسعه داده اند که می تواند سن ظاهری یک شخص را در تصاویر تغییر دهد و در عین حفظ هویت شناسایی بیومتریک منحصر به فرد آن شخص باشد. این پیشروانه می تواند کاربردهای مختلفی در حوزه هایی مانند سرگرمی، کاربردهای کفیری و تبلیغات شخصی داشته باشد. محققان مدل خود را با استفاده از یک مجموعه کوچکی از تصاویر هر شخص و همراه با مجموعه جداگانه ای از تصاویری که رقم سن شخص را نشان می دهند، آموزش دادند. مدل قادر است به سناریوهای پیری یا

چهره فرد از طریق شناسایی چهره با هوش مصنوعی اسکن شده و با عکس موجود در سند هویت فرد تطبیق داده می شود. آزمایش تشخیص زنده بودن نهایی، ویژگی های عضلات صورت کاربر را تجزیه و تحلیل می کند. همچنین هوش مصنوعی برای جعل صورت بگیرد سیستم آن را تشخیص داده و تأیید ناموفق خواهد بود



اخبار مربوط به بد اخلاقی هایی که با کمک هوش مصنوعی شکل گرفته روبرو افزایش است و این در حالی است که بسیاری از کاربران مطلع نیستند که ماشین های هوش مصنوعی تولید می کنند و خود نیز به این چرخه کمک می کنند.

اخیراً خبرهای ریزو درستی از کاربران در شبکه های اجتماعی منتشر می شود که به اذعان خود کاربر غیر واقعی و جعل شده است. به عنوان مثال داستان چند دختر نوجوان که با تصویرسازی از آنها با لباس نامناسب و قرار دادن در شبکه های اجتماعی مشکلاتی را در زندگی شخصی آنها به وجود آورده بود. این دختران اذعان کرده اند که در آن موقعیت مکانی با آن وضعیت ظاهری حضور نداشته اند و اینها جعل است. اما چه کسی دست به جعل می زند و داستان از چه قرار است و در کل چگونه می توان پی برد محتوایی جعلی است؟

حتماً تحولات هوش مصنوعی را شما نیز درک کرده اید. هوش مصنوعی از یادگیری ماشین و آموزش مدل ها استفاده می کند. دستگاه از طریق داده هایی که در گذشته دریافت کرده یاد می گیرد و سپس بر اساس الگوی داده های قبلی بر اساس پیش بینی ها و احتمالات تصمیم گرفته و کار می کند. این یادگیری در یک سال گذشته به حدی با جهش همراه بوده که حتی نگرانی خود دانشمندان را به دنبال داشته است. تا جایی که یکی از این نگرانی ها برنامه های جدید در تغییر هویت افراد است که می تواند بدون کوچکترین تردیدی تصویری جدید از فرد ارائه دهد.

### سن و نژاد خود را تغییر دهید

نمونه ای از این برنامه ها که در ظاهر برای صنعت سینما یا سرگرمی استفاده می شود اشاره به این مهم دارد که هوش مصنوعی قادر به تغییر هویت واقعی آدم ها است.

به عنوان مثال نسخه آزمایشی فناوری که استودیو پانوراما، کمپانی سازنده جلوه های بصری IP و توسعه فناوری، آن را عرضه کرده، همه را شگفت زده کرده است. استودیو پانوراما فرایند ارائه کرده است که می تواند به صورت کلی نژاد افراد را تغییر دهد. هیچ کس واقعاً نمی داند که این استودیو به کمک کدام فناوری کار خود را پیش برده است. بعضی از افراد خبره در این حوزه حدس می زنند از ابزار محبوب Stable Diffusion دیگر شبکه های عصبی مصنوعی کمک گرفته شده باشد. سؤالی که پیش می آید این است که این قابلیت جدید برای تغییر نژاد افراد در فیلم ها، سریال های تلویزیونی یا حتی ویدیو هایی که در رسانه های اجتماعی منتشر می شوند، چگونه بر جامعه تأثیر می گذارد؟ جواب هرچه که باشد، این فناوری یک قدم دیگر در پوشاندن واقعیت های زندگی افراد گام برمی دارد.

از طرفی تغییر چهره با هوش مصنوعی، یکی از کاربردهای جالب این فناوری محسوب می شود که می تواند در برخی شرایط خاص، بسیار حساسیت زا باشد. برای مثال ویژگی مذکور به تولیدکنندگان محتوا و فعالان شبکه های اجتماعی، امکان ساخت ویدیوهای جذاب تر را



محققان مدرسه مهندسی تاندون دانشگاه NYU

یک تکنیک هوش مصنوعی جدید توسعه داده اند که

می تواند سن ظاهری یک شخص را در

تصاویر تغییر دهد و در عین حفظ هویت

شناسایی بیومتریک منحصر به فرد آن

شخص باشد. این پیشروانه می تواند

کاربردهای مختلفی در حوزه هایی مانند

سرگرمی، کاربردهای کفیری و تبلیغات شخصی داشته باشد