اگه میتونی منو بگیر!

Catch Me If You Can!

امیرحسین فروغی
دانشجو کارشناسی علوم کامپیوتر دانشگاه صنعتی امیرکبیر
Ah.foroughi98@gmail.com

چکیده

امروزه مرزهای تکنولوژی و فناوری بسیار فراتر از آنچه تصور می‌شود، گسترده شده است. اگر در گذشته تنها ممکن بود عکس افراد توسط نرم افزارهای مختلف گرافیکی دستکاری شود و چیزی خلاف واقعیت را به بیننده نشان دهد، امروز با فناوری خطرناک‌تری روبه‌رو هستیم که می‌تواند چهره و صدای شما را به طرز شگفت‌آوری تقلید کرده و در قالب ویدیوهای غیرواقعی منتشر کند.

دیپ‌فیک (Deepfake) یا همان جعل عمیق، ترکیبی از دو واژه deep learning (یادگیری عمیق) و fake (جعلی)، فناوری جدیدی بر مبنای هوش مصنوعی است که به واسطهٔ آن تصاویر و ویدیوهای دروغین اما واقع‌گرایانه ساخته می‌شود و می‌تواند هر بیننده‌ای را تحت تأثیر خود قرار دهد.

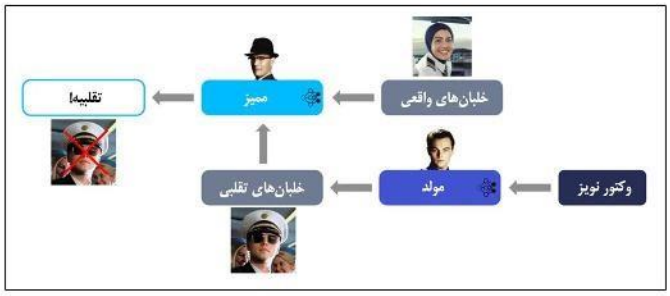
کلمات کلیدی: دیپ فیک- تکنولوژی- الگوریتم شبکهٔ مولد تخاصمی

مقدمه

با توجه به توسعه و پیشرفت تکنولوژی و ترویج استفاده از شبکه‌های اجتماعی مسئلهٔ روبه‌رو شدن با محتواهای مختلف به وجود می‌آید. در این بین بعضی افراد با استفاده از این بستر و تولید بعضی محتواهایی که غالباً ساختگی هستند درصدد سوءاستفاده از این محیط برآمدند. در این مقاله به معرفی یکی از جدیدترین تکنولوژی‌هایی که در این زمینه استفاده می‌شود و از زمان پیدایش آن زمان زیادی نمی‌گذرد، می‌پردازیم. با استفاده از این تکنولوژی می‌توان محتواهایی را تولید کرد که قبلا هیچ سابقه‌ای در تاریخ نداشته‌اند و هیچ تصوری درباره آن‌ها نداشته‌ایم؛ مثلا تولید تصاویر افرادی که وجود خارجی نداشته‌اند.

دیپ‌فیک چگونه ساخته می‌شود؟

چندین راه برای ساخت ویدئوهای دیپ‌فیک وجود دارد؛ اما در تمام این راه‌ها، باید مقدار زیادی از داده را به مدل‌های یادگیری ماشین تغذیه کرد تا از این طریق محتوای جعلی تولید شود. واقع‌گرایانه‌ترین نمونه‌های ساخته‌شده، حجم عظیمی از داده‌های صوتی، تصویری و ویدئویی را طلب می‌کنند. الگوریتم شبکهٔ مولد تخاصمی[1] یا به‌طور خلاصه، گن (GAN)، دارای یک بخش «مولد» و یک بخش «ممیز» است؛ مثلا فرض کنید گن قصهٔ ما، یاد گرفته باشد تصویرهای دروغین از خلبان‌ها بسازد. مولد سعی می‌کند عکس‌های تقلبی جعل کند. از آن طرف ممیز، عکس‌های جعلی ساخت مولد و عکس‌های واقعی را کنار هم می‌گذارد و به خودش یاد می‌دهد که عکس واقعی را از دروغین تشخیص دهد. هرچقدر که مدل گن بیشتر یاد بگیرد، هر دو بخش‌های مولد و ممیز هم در کارشان بهتر عمل می‌کنند و هرکدام باعث می‌شود دیگری در کار خودش ماهرتر شود. دیپ‌فیک‌ها جعل‌هایی هستند که مولد بالاخره توانسته از زیر دماغ ممیز رد کند!



ساختار و روند کلی شبکه‌های مولد تخاصمی

در واقع این فناوری که برای ایجاد محتوای صوتی و تصویری متقاعد کننده و درعین‌حال غیرواقعی ساخته شده، به‌سرعت در حال رشد و بهبود است و انتظار می‌رود روزبه‌روز استفاده از آن گسترده‌تر شود. برنامه‌های ویرایش تصویر نظیر فتوشاپ، سال‌هاست کاری مشابه را از طریق جعل کردن تصاویر انجام می‌دهند؛ اما چیزی که اکنون با آن روبه‌رو هستیم، مبحثی کاملا متفاوت و نگران‌کننده‌تر از جعل عکس یک نفر در فتوشاپ است.

با پیشرفت خیره‌کننده هوش مصنوعی طی سال‌های اخیر، بسیاری از کارهایی که در گذشته سخت و ناممکن به نظر می‌رسیدند، ممکن شده‌اند. پیش‌تر، کمتر کسی فکر می‌کرد که روزی بتوان محتوای یک ویدئو را به‌طورکلی و بدون دخالت مستقیم انسان تغییر داد؛ اما اکنون دیپ‌فیک ثابت کرده که چنین باوری در دنیای امروز جایی ندارد و به راحتی می‌توان ویدئوهایی تولید کرد که به سبب واقع‌گرایانه‌بودن، نتوان میان حقیقت و دروغ آن‌ها تمایزی قائل شد.

[1] Generative Adversarial Network

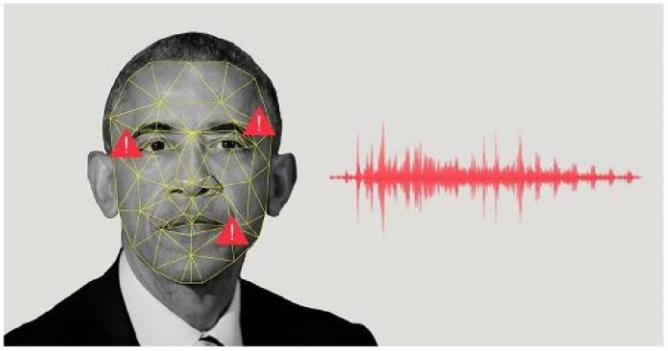
جایگذاری عکس یک نفری به‌عنوان شخصی دیگر

همان‌طور که پیش‌تر اشاره شد، دیپ‌فیک یک تکنیک مبتنی بر هوش مصنوعی است؛ بنابراین نیازی به دخالت مستقیم انسان ندارد؛ ازاین‌رو هرکسی از طریق دیپ‌فیک می‌تواند ویدئویی جعلی و درعین‌حال واقع گرایانه بسازد.

حتی در این زمینه ابزارهایی نیز ساخته شده‌اند تا فرایند ساخت چنین ویدئوهایی ساده‌تر شود؛ به‌عنوان نمونه می‌توان به موتور جستجویی اشاره کرد که تصویر اشخاص عادی جامعه را دریافت می‌کند و بر اساس آن شبیه‌ترین بازیگر فیلم‌های بزرگ‌سالان را پیشنهاد می‌دهد تا از ویدئوهای وی برای ساخت محتوای غیراخلاقی دروغین با چهره فرد موردنظر استفاده شود.

دیپ‌فیک و سقوط اخلاقیات

امروزه ویدیوهای دیپ‌فیک بسیاری از هنرمندان و افراد مشهور ساخته می‌شود و بیننده بدون آنکه متوجه عدم صحت و واقعیت آن‌ها شود، محتوای آن‌ها را باور کرده و به انتشارشان در فضای مجازی دست می‌زند. در نتیجه با توجه به پیشروی بدون محدودیت اینِ فناوری، باید گفت که به‌زودی تشخیص بین مرز حقیقت و دروغ کاملا غیرممکن می‌شود. فناوری دیپ‌فیک در طول ظهور و پیدایش خود، نه‌تنها جامعهٔ بازیگران و سلبریتی‌ها را هدف گرفته بلکه به حریم چهره‌های بزرگ سیاستمدار نیز تجاوز کرده است. به‌عنوان‌مثال چندی پیش ویدیویی از باراک اوباما منتشر شد که در آن دونالد ترامپ را فردی حقیر و غیرمنطقی خطاب می‌کرد. اگرچه این ویدیو صحت نداشت و کاملا غیرواقعی بود اما افراد زیادی در ابتدا آن را باور کردند و به انتشار آن در فضای مجازی اقدام کردند. در همین راستا رئیس‌جمهور سابق آمریکا، باراک اوباما، در خصوص تکنولوژی دیپ‌فیک اظهارنظر کرد و ابراز داشت در دنیایی که می‌توانند به‌سادگی صحبت‌ها و ویدیوهای غیرواقعی از من ساخته و منتشر کنند، به مرحله‌ای خواهیم رسید که تشخیص مرز بین واقعیت و دروغ بسیار مشکل خواهد شد و این مطمئنا بر پایه‌های دموکراسی ما که بر مبنای حقیقت است، تأثیر خواهد گذاشت.



یکی از اولین ویدیوهایی که با استفاده از این تکنولوژی ساخته شد و در شبکه‌های اجتماعی پخش شد ویدیویی از اوباما بود که درباره دونالد ترامپ حرف‌های تندی زده بود

متأسفانه گسترش این موضوع باعث شده است تا عده‌ای از این راه کسب درآمد کنند. در انجمن‌های اینترنتی، عده‌ای بابت ساخت ویدئوهای غیراخلاقی از فرد موردنظرشان، قیمت‌های بالایی پرداخت می‌کنند. طبق یافته‌های واشنگتن‌پست تنها در یک مورد، شخصی نزدیک به ۵۰۰ عکس از چهرهٔ فرد موردنظرش را در یکی از این انجمن‌ها آپلود کرد؛ فردی که بابت کار با کیفیت، پول خوبی نیز پرداخت می‌کرد. موضوع تأسف برانگیز این است که تاکنون هیچ قانونی برای توسل قربانیان به آن، تدوین نشده است.

همان‌طور که مشاهده کردید در آینده‌ای نه چندان دور و با گسترش فناوری دیپ‌فیک، عملاً تشخیص بین مرز حقیقت و دروغ غیرممکن خواهد شد. علاوه بر این تولید و فراگیر شدن نرم‌افزارهای تغییر چهرهٔ مبتنی بر دیپ‌فیک نیز هشداری جدی بر نقض حریم خصوصی کاربران هستند. باید منتظر ماند و دید که پیشرفت بی‌مهابای فناوری تا کجا بر زندگی افراد تأثیر خواهد گذاشت.

در این میان، شبکه‌های اجتماعی بزرگ نظیر فیس‌بوک که نقش پررنگی در انتقال اخبار دارند، هیچ عکس‌العملی را نسبت به محتوای دیپ‌فیک نشان نداده‌اند؛ امری که نگرانی‌ها دربارهٔ گسترش چنین پدیده‌ای را بیش از پیش تشدید می‌کند.

چنین اتفاقی نه‌تنها اطلاعات نادرست را در سطح جامعه گسترش می‌دهد بلکه پذیرش حقیقت را توسط افراد به امری سخت و ناممکن تبدیل می‌سازد. تصور کنید شبکه‌های اجتماعی پر از ویدئوهای جعلی و دروغین باشد، رهبران سیاسی کشورها حرف‌های پیشین خود را

تکذیب کنند و افراد جامعه همواره نگرانی سوءاستفاده از تصاویرشان را با خود به همراه داشته باشند. در این صورت با جامعه‌ای بیمار و بدگمان روبه‌رو خواهیم شد که به همه‌چیز مشکوک است، سخنان رهبرانش را باور ندارد و از آن‌سو رهبران سیاسی کشورها نیز به‌سادگی و با پناه بردن به واژهٔ دیپ‌فیک، نه‌تنها هیچ انتقادی را نمی‌پذیرند بلکه حرف‌های واقعی خود را نیز تکذیب می‌کنند تا از زیر بار مسئولیت شانه خالی کنند. در چنین جامعه یا بهتر است بگوییم چنین جهانی، دیگر مرزی بین حقیقت و دروغ باقی نمی‌ماند، «اعتماد» به واژه‌ای بس مضحک تبدیل می‌شود و دروغ، خوراک روزانهٔ همگان خواهد شد.

هوش مصنوعی شبه‌انسانی و تعاملات ارتباطی نو

جهان پر از دیپ‌فیک شاید مخوف و ناامن باشد؛ اما این تنها آیندهٔ ممکن نیست! دیپ‌فیک کاربردهای مثبتی هم دارد؛ این فناوری می‌تواند نحوهٔ ارتباطات را دگرگون کند و شکل‌های کاملا جدیدی از آن به وجود بیاورد. به‌عنوان‌مثال تصور کنید فناوری تولید صدا با فناوری دیپ‌فیک ترکیب شود! در آینده‌ای نه‌چندان دور، سخنگوهای هوشمندی خواهیم داشت که نه‌تنها می‌توانند با صدای خواننده‌های موردعلاقه‌مان صحبت کنند که بلدند وقتی خودمان سرکار نیستیم، به جای ما تماس‌های تلفنی را جواب بدهد!

جمع‌بندی

در چنین جهانی با هر دروغی که می‌گوییم، دیگر دینی به حقیقت نخواهیم داشت؛ زیرا دیگر حقیقتی باقی نمی‌ماند که بخواهد روزی از میان خرابه‌های تمدن به‌ظاهر انسانی سر به بیرون بیاورد. مهم نیست دیپ‌فیک‌ها چقدر واقع‌گرایانه‌تر شوند یا دقت فناوری‌های ضد دیپ فیک تا چه حد افزایش پیدا کند؛ آسیب اصلی ناشی از این دیپ‌فیک‌ها کار انسان‌هایی هست که آن‌ها را می‌سازند، ساخته‌های دروغین را باور می‌کنند و چیزی که بدون تحقیق، درست فرض کرده‌اند را نشر می‌دهند. به جای اینکه انگشت اتهام را به سمت خود فناوری دیپ‌فیک بگیریم، باید ببینیم چطور می‌شود کاری کرد که افراد در مورد چیزهایی که در اینترنت می‌بینند با دید منتقدانه‌تری قضاوت کنند و هنگام به اشتراک گذاری در شبکه‌های اجتماعی هوشمندانه‌تر عمل نمایند. اثرات منفی دیپ‌فیک را نمی‌شود انکار کرد؛ اما باید نگاهمان را به بخش‌های مثبت‌تر هوش مصنوعی بدوزیم و پتانسیلی که دیپ‌فیک برای ایجاد روش‌های ارتباطی جدید و بهتر کردن زندگی‌هایمان دارد را به مسیر درست هدایت کنیم. اکنون باید این سوال را پرسید که آیا پیشرفت لجام‌گسیخته و بی‌مهابای فناوری در تمامی زمینه‌ها، ارزش این را خواهد داشت تا پایه‌های جامعهٔ خود را نابود سازیم و آینده را بر ویرانه‌های تمدن بشری نظاره‌گر باشیم؟

منابع

Nahua Kang.(2019) Deepfake: The Good, The Bad and the Ugly (Medium)