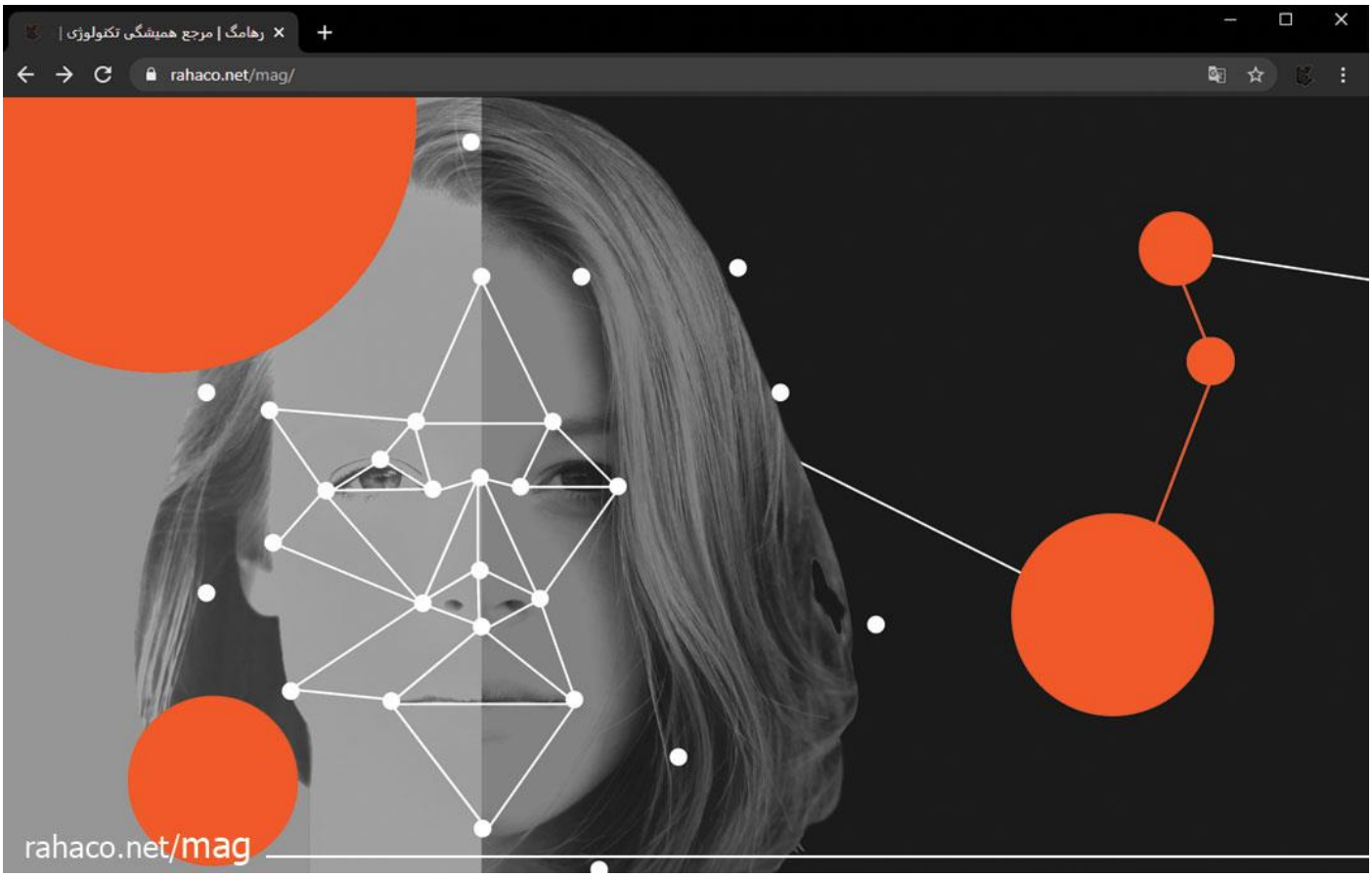
مرز باریک میان دیپ فیک و واقعیت

مجموعه شرکت‌های دانش بنیان رها

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net



فهرست

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

در طول چند دهه گذشته، هوش مصنوعی به سرعت در حال توسعه بوده است. این تکنولوژی برنامه‌هایی در زمینه‌های مختلف و برای اهداف بی‌شمار ارائه داده‌است که باعث بهبود کیفیت و کارایی صنایع مختلف می شود. اما همه محصولات هوش مصنوعی تأثیر مثبتی بر جامعه ندارند؛ گاهی اوقات این فناوری‌ها مورد سوءاستفاده قرار می‌گیرد. نمونه‌ای از این فناوری به نام دیپ فیک (Deepfake) شناخته می‌شود.

با تکنولوژی دیپ فیک می‌توانید چهره یک فرد را با چهره فرد دیگر، چه در یک تصویر یا چه در ویدیو، جایگزین کنید. قربانیان چنین اقداماتی اغلب افراد مشهور، سلبریتی‌ها و سیاستمداران هستند. این مقاله توضیح می‌دهد که این فناوری بر چه اساسی به وجود آمده‌است و چه روش‌هایی برای تشخیص آن وجود دارد.

دیپ فیک چیست؟

کلمه "Deepfake" ترکیبی از دو کلمه "عمیق" و "جعل" است. دیپ در اینجا به عنوان یادگیری عمیق شناخته می‌شود. فناوری دیپ فیک در رسانه‌ها برای ایجاد محتوای جعلی، جایگزین یا ترکیب چهره ها، تغییر گفتار و دستکاری احساسات استفاده می‌شود. اولین قدم ها به سمت این فناوری در دهه 90 توسط موسسات دانشگاهی انجام شد و بعدها مخاطبان بیشتری به آن روی آورده‌اند. اگرچه دیپ فیک در صدر اخبار تکنولوژی نیست، اما با این وجود توانسته سر و صدای زیادی در فضای مجازی و رسانه‌ها ایجاد کند.

دیپ فیک چگونه کار می‌کند؟

استراتژی‌های بسیاری برای ساخت نرم افزار دیپ فیک با استفاده از الگوریتم‌های یادگیری ماشین وجود دارد. به بیانی ساده، این الگوریتم‌ها می‌توانند بر اساس داده‌های ورودی محتوا تولید کنند. البته، ایجاد یک چهره جدید در این برنامه یا جایگزینی بخشی از چهره باید آموزش داده شود. این برنامه با استفاده از داده‌های بسیار زیاد، داده‌هایی جدید برای خود می‌سازد. اساسا این داده‌ها بر اساس رمزگذارهای خودکار و گاهی اوقات بر روی شبکه‌های مولد تخاصمی (GAN) هستند. حال بیایید ببینیم که این روش‌ها چگونه کار می‌کنند؟

رمزگذارهای خودکار:

رمزگذارهای خودکار خانواده‌ای از شبکه‌های عصبی تحت نظارت خود هستند. آن‌ها فقط مختص داده‌ها می‌باشند، به این معنی که رمزگذاری خودکار می‌تواند داده‌ها را مشابه آنچه که آموزش دیده‌اند، فشرده کنند. علاوه بر این، خروجی رمزگذار خودکار با ورودی آن یکسان نخواهد بود. رمزگذار خودکار از 3 جزء تشکیل شده‌است: رمزگذار، کد و رمزگشا. رمزگذار داده‌های ورودی را فشرده می‌کند و پس از اینکه رمزگشا کد ورودی را بازسازی کرد، کد تولید می‌شود. انواع مختلفی از رمزگذار خودکار وجود دارد: رمزگذار خودکار حذف نویز، رمزگذار خودکار عمیق، رمزگذار خودکار کانولوشن و غیره.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

شبکه‌های مولد تخاصمی (GAN):

گان رویکردی برای مدل‌سازی مولد از داده‌های ورودی است؛ یعنی از داده‌های ورودی به منظور تولید داده‌های جدید استفاده می‌شود. این سیستم توسط دو شبکه عصبی متمایز آموزش داده می‌شود: یک مولد و یک تفکیک کننده. مولد الگوهای موجود در مجموعه داده‌های ورودی را کشف کرده و آن‌ها را بازتولید کند. سپس داده‌های تولید شده همراه با داده‌های واقعی برای ارزیابی به تفکیک کننده ارسال می‌شود. در اینجا هدف مولد فریب دادن تفکیک کننده است. این سیستم تا جایی ادامه می‌یابد که تفکیک کننده دیگر داده‌های تولید شده را با داده‌های واقعی اشتباه نگیرد. هرچه تشخیص داده‌های تولید شده از داده‌های واقعی سخت‌تر باشد، کارایی آن بهتر خواهد بود. آموزش GAN ها به مراتب سخت تر است و به منابع بیشتری نیاز دارد. از آن‌ها بیشتر برای تولید عکس به جای فیلم استفاده می‌شود.

آیا دیپ فیک خطرناک است؟

دیپ فیک یکی از خطرناک ترین محصولات هوش مصنوعی شناخته می‌شود. بیشتر برنامه‌های آن در دنیای واقعی برای اهداف دزدی یا کلاهبرداری استفاده می‌شوند. یکی از اولین موارد کلاهبرداری دیپ فیک در بریتانیا اتفاق افتاد. کلاهبرداران با مدیر عامل یک شرکت انرژی تماس گرفتند و با جعل صدای رئیس آلمانی او، به او دستور دادند 220000 یورو به یک حساب بانکی منتقل کند. ممکن است نتیجه نهایی دیپ فیک از واقعیت قابل تشخیص نباشد و همین ویژگی آن را به یک سلاح عالی برای کلاهبرداران تبدیل می‌کند.

تاثیر دیپ فیک بر جامعه

اگر این تکنولوژی به دست افراد نادرست برسد می‌تواند منجر به هرج و مرج شود. از آنجا که بخش بزرگی از جامعه ما از رهبران، سلبریتی‌ها و اینفلوئنسرها ساخته شده‌است، اطلاعات نادرست و جعلی می‌تواند نظر مردم را راجع به آن‌ها تغییر دهد. این موضوع حتی چندین رئیس جمهور ایالات متحده را نیز درگیر کرد. اخبار جعلی مربوط به رهبران سیاسی می‌تواند اعتبار کشور را تضعیف کند و منجر به از دست دادن اعتماد مردم به آن‌ها شود.

آیا تکنولوژی دیپ فیک قانونی است؟

از آنجایی که دیپ فیک در چند سال اخیر شروع به گسترش کرد، قوانین مربوط به کاربرد آن هنوز با این فناوری مطابقت نکرده‌است. در بسیاری از کشورها به هیچ‌وجه مقرراتی درباره استفاده از آن وجود ندارد. یکی از کشورهایی که در آن قانون استفاده از دیپ فیک وجود دارد، چین است. اداره فضای مجازی چین اعلام کرد که هرگونه اخبار جعلی که با استفاده از دیپ فیک منتشر می‌شود غیرقانونی است. در ایالات متحده، اگر دیپ فیک بر علیه نامزدهای شرکت کننده در مناصب دولتی ساخته شود، جرم تلقی می‌شود.

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

دیپ فیک در جهان امروز

گسترش دیپ فیک با فیلم‌های جعلی سلبریتی‌ها آغاز شد. بسیاری از سلبریتی‌های زن قربانی این تکنولوژی جدید شده‌اند. از جمله جنیفر لارنس، اما واتسون و گال گدوت. این موضوع زنان سیاستمدار کشورهای مختلف را نیز تحت تاثیر قرار داد، مانند: میشل اوباما، ایوانکا ترامپ و کیت میدلتون.

گروه بعدی از افرادی که تحت تأثیر دیپ فیک قرار می‌گیرند، سیاستمداران هستند. ویدئوهایی از اوباما در حال توهین به ترامپ وجود منتشر شد. در ویدئویی دیگر، صحبت‌های نانسی پلوسی طوری درست شد تا حضار باور کنند که او مست بوده‌است. در ویدئوی جعلی دیگر، ترامپ کشور بلژیک را به دلیل عضویتش در توافقنامه آب و هوایی پاریس مسخره می‌کند.

لازم به ذکر است که موارد استفاده قانونی از دیپ فیک نیز وجود دارد. درواقع، این عقیده وجود دارد که دیپ فیک آینده تولید محتوا است.

کانال MBN کره جنوبی با استفاده از دیپ فیک یک مجری جایگزین برای اخبار خود ساخت!

تشخیص دیپ فیک

فناوری هایی که دیپ فیک را تشخیص می‌دهند نیز بر اساس هوش مصنوعی و با استفاده از همان الگوریتم‌هایی که برای ساخت دیپ فیک استفاده می‌شوند، ساخته شده‌اند. آن‌ها علائمی را تشخیص می‌دهند که در عکس‌ها یا فیلم‌های واقعی وجود ندارند. در ابتدای کار، پلک زدن غیرواقعی یا پلک نزدن نشانه خوبی از دیپ فیک بود. اما با گذشت زمان، سیستم‌ها یاد گرفته‌اند که پلک زدن جعلی را نیز بسازند. علائم تشخیص دیپ فیک عبارتند از:

- رنگ غیر واقعی پوست یا تغییر رنگ پوست
- حرکات تند و سریع
- همگام سازی ضعیف صحبت با حرکت لب
- چهره فرد مبهم‌تر از تصویر پس‌زمینه است.
- پیکسل‌های اضافی در قاب

نتیجه گیری

دیپ فیک یک فناوری امیدوارکننده است. بشر در حال شناخت است و هنوز کاربرد کامل آن را در جامعه پیدا نکرده‌است. مانند بسیاری از فناوری‌ها، دیپ فیک نیز مزایا و معایب خود را دارد؛ یعنی می‌تواند به دنیای ما آسیب

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net

برساند یا باعث بهبود آن شود. هنوز به زمان نیاز داریم تا بفهمیم چگونه از آن در صنایع مختلف نهایت استفاده را ببریم. با گذشت زمان راه‌های زیادی برای کنترل این تکنولوژی جدید به وجود خواهد آمد.

هنر تکنولوژی را به چالش می کشد و تکنولوژی به هنر الهام می بخشد

آدرس: تهران،خیابان سپهبد قرنی،خیابان دهقانی،پلاک ۱۲کدپستی۱۵۸۳۶۱۶۴۱۴ تلفن :۰۲۱۵۴۵۲۱
www.rahaco.net