



یادداشت:

دکتر مهدی زارع

استاد پژوهشگاه بین‌المللی  
زلزله‌شناسی و مهندسی زلزله

به مناسبت ۱۳ اکتبر

روز جهانی کاهش سوانح طبیعی

## مدیریت بحران

## در تهران برای زلزله بزرگ

📍 ریسک زلزله شدید در تهران به دلیل وجود بافت فرسوده و جمعیت زیاد و همچنین نزدیکی به پهنه گسل‌های فعال در شهر تهران در این نواحی به نسبت بالاتر است؛ مناطق ۱۲ و ۱۶ شهرداری و منطقه راه‌آهن، محور خیابان انقلاب و آزادی، ارگ قدیم تهران حد فاصل خیابان شوش، هفده شهریور، انقلاب و کارگر جنوبی و بازار تهران، خیابان مولوی، میدان بهارستان، میدان امام خمینی، محله امیریه و خیابان جمهوری اسلامی. بر اساس آخرین سرشماری سال ۱۳۹۵، در شمال تهران ۱/۱ میلیون نفر در محور مرکز به سمت جنوب تهران (در مناطق ۸ تا ۲۱ شهرداری تهران) حدود پنج میلیون نفر در نزدیکی پهنه‌های گسل‌های فعال زندگی می‌کنند، البته این تنها ریسک مرتبط با زلزله برای شهر تهران نیست و فقط برآوردی از جمعیت ساکن در «پهنه‌های گسل در شمال و جنوب شهر» را نشان می‌دهد و بدیهی است موضوع تراکم بالای جمعیت و بافت فرسوده به‌ویژه در مناطق ۱۲، ۱۴، ۱۵، ۱۶ و ۱۷ تهران خود مسأله‌ای جداگانه است. جنبش شدید در محدوده پهنه گسل و در بافت‌های فرسوده حدود ۵/۳ میلیون نفر، یعنی ۵۶ درصد جمعیت تهران را شامل می‌شود.

زمین‌لرزه‌های مخرب تاریخی در ناحیه شهری سال ۳۲۰ قبل از میلاد مسیح و همچنین زلزله‌های تاریخی سال‌های ۷۴۳، ۸۵۵، ۹۵۸ شهری و ۱۸۳۰ میلادی دماوند-شمرانات‌واز سوی دیگر رخداد زلزله‌های مهم ۱۱۷۲ و ۱۹۶۲ میلادی بونین زهر در جنوب دشت قزوین در غرب تهران که برآورد می‌شود همگی بزرگایی بیش از هفت داشته‌اند، نمایانگر احتمال رخداد زلزله‌های مخرب در ناحیه شهری یا در نزدیکی گستره شهر تهران است. این درحالی است که گسل شمال تهران با جابه‌جاکردن نهشته‌های کواترنر در ناحیه شمالی تهران همراه بوده و آخرین بررسی‌های دیرینه لرزه‌شناسی گویای لرزه‌زا بودن آن حتی در مدت زمان عهد حاضر- هولوسن- بوده است.

شبکه لرزه نگاری محلی داخل شهر تهران از خرداد ۱۳۸۲ از سوی سازمان پیشگیری و مدیریت بحران شهر تهران راه‌اندازی شده و با ۱۲ ایستگاه در حال ثبت زلزله‌های محلی با کیفیت بالاست. زلزله‌های ثبت‌شده در این شبکه بیشتر لرزه‌خیزی طبیعی در شرق تهران و محدوده شرقی گسل شمال تهران و قطعه شرقی‌گسل مشا و منطقه‌کوه‌بی‌ب‌شهربان‌در راستای گسل ایوانکی‌را شاخص نشان می‌دهد. در پایان نامه دکتری خانم فراهانی که از دانشجویان سابق دکتری نگارنده بود و روی لرزه‌خیزی ثبت شده در همین شبکه محلی تهران طی سال‌های ۱۳۸۸ تا ۱۳۹۱ کار کرده بود معلوم شد در بازه مورد مطالعه ۱۳۸۳ تا ۱۳۸۹ لرزه‌های کمی در مجاورت گسل‌های طالقان، کهریزک و قطعه مرکزی گسل شمال تهران ثبت شده است. در عوض لرزه‌خیزی مهمی در امتداد گسل‌های مشا، گرمسار و کندوان مشاهده شد. لرزه‌خیزی قابل‌توجهی نیز در امتداد قطعه شرقی گسل مشا به‌ویژه در مجاورت شهرهای دماوند، پردیس و منطقه شرق لوسانات ثبت شد. از سوی دیگر قطعه مرکزی گسل مشاء (از لوسانات تا میگون و شهرستانک) به احتمال زیاد چون قطعه‌ای از یک‌گسل فعال (گسل‌مشاء) قفل شدگی دارد

پس در سکوت لرزه‌ای به‌سرمی‌برد. نتایج مطالعه نگارنده سال ۱۳۷۴ روی قطعه شرقی گسل مشاء نشان داد این گسل باعث لغزش سالانه چهارمیلی‌متر به‌صورت عمودی و دومیلی‌متر به‌صورت افقی(امتداد لغز) می‌شود. دکتر شهریار سلیمانی در پایان نامه‌دکترای خود نشان داد قطعه شرقی گسل مشاء در ۱۰هزار سال گذشته ۹ زلزله ویرانگر و مخرب داشته است. به این ترتیب هم بخش شرقی و هم بخش مرکزی گسل مشاء می‌تواند باعث بروز زلزله‌هایی با بزرگی بیشتر از ۷ شود. اکنون اولین‌اولویت در کاهشریسک‌ومدیریت بحران در تهران، سبک‌سازی جمعیت‌در معرض آسیب در منطقه تهران و پیرامون است. 📍

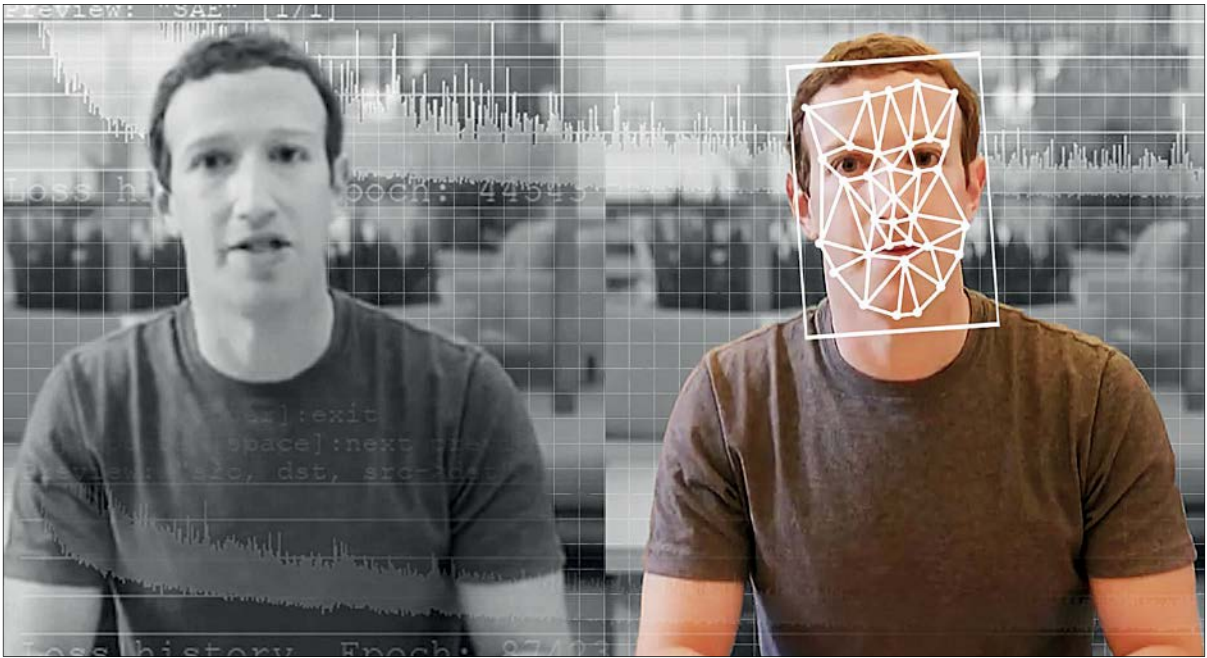


## نرم افزار همراهی که عیب موتور خودرو را پیدا می‌کند

شرکت اشکودا نرم‌افزار همراهی ابداع کرده که می‌تواند به موتور خودرو گوش و هر گونه اختلال در آن را ردیابی کند. متخصصان می‌توانند گوش هوشمند را نزدیک موتور روشن خودرو نگه دارند. میکروفن گوشی صدای خودرو را ضبط می‌کند و در مرحله بعد هوش مصنوعی فایل‌های صوتی را با اطلاعات ذخیره شده در مخزن خود مقایسه می‌کند. دقت این اپلیکیشن هم اکنون ۹۰ درصد اعلام شده و می‌تواند ۱۰ الگو از جمله اختلالات مربوط به کمپرسور تهویه هوا، دنده و کلاچ در جعبه گیربکس را شناسایی کند. / مهر

در پی انتشار ویدئویی در فضای مجازی از خواندن ترانه «ایران من» بالبخوانی جمعی از چهره‌های مشهور تاریخ معاصر ایران که با فناوری «جعل عمیق» ساخته شده بود، به ابعاد گوناگون کاربردهای این فناوری می‌پردازیم

# دیگر به چشمتان هم اعتماد نکنید!



مارک زاکربِrg، مالک فیسبوک که همواره متهم به سرقت اطلاعات کاربران این شبکه اجتماعی می‌شود از رایج‌ترین سوزه‌ها برای ساخت ویدئوهای جعل عمیق است



ویدئوی جعل

عمیق ترانه

«ایران من»

همایون شجریان

را با اسکن این کد

در گوشی

هوشمندتان

تماشا کنید

### آیا جعل عمیق می‌تواند ویرانگر باشد؟

با روند فعلی باید منتظر جعل عمیق‌های بیشتری باشیم که قصدشان آزار رساندن، ترساندن، تحقیرکردن، بی‌اعتبارسازی و ایجاد بی‌ثباتی است. اما آیا جعل عمیق در عرصه بین‌المللی نیز خطرناک است؟ در این مورد وضعیت مشخص نیست. اما آنچه مشخص است این که یک ویدئوی جعل عمیق از رهبران مهم دنیا یا تصاویر جعلی که تجمع نیروهای نظامی را در مرزها نشان می‌دهد، جنجال غیرقابل کنترلی به پا نخواهد کرد و در بیشتر کشورها مردم به دستگاه امنیتی خود اعتماد دارند. اما به‌رحال قابلیت‌های این فناوری فضای کافی برای آشوب‌آفرینی را دارد. آیا جعل عمیق می‌تواند قیمت سهام را تغییر دهد یا بر رای‌دهنده‌ها تاثیر بگذارد یا به تنش‌های مذهبی دامن بزند؟ به‌لکه ممکن است، اما بهتر است امیدوار باشیم با افزایش آگاهی عمومی این موارد قابل کنترل خواهد بود و خطر زیادی نخواهد داشت.

### آیا اعتماد به مستندات از بین می‌رود؟

در جامعه‌ای که مردم نمی‌توانند یا این زحمت را به خود نمی‌دهند که اخبار درست را از اخبار جعلی تمایز کنند، تاثیرات توطئه‌آمیز جعل عمیق در کنار اخبار جعلی، به گسترش بی‌اعتمادی در جامعه دامن می‌زنند. وقتی اعتماد از بین برود، ایجاد شبهه در مورد وقایع خاص آسان‌تر خواهد بود. با دسترسی بیشتر به این فناوری، جعل عمیق می‌تواند مشکلات زیادی را در دادگاه‌ها به وجود آورد. به‌ویژه در مورد پرونده‌های اخذ حضانت فرزندان و شرکت‌های بیمه که اتفاقات غیرواقعی ممکن است به عنوان شاهد به دادگاه ارائه شوند. جعل عمیق حتی می‌تواند امنیت اشخاص را نیز تهدید کند. جعل عمیق با تقلید از اطلاعات زیست‌سنجی (بیومتریک)، هر سامانه‌ای را که متکی به تشخیص چهره، صدا، رگ‌های خونی چشم یا نحوه راه‌رفتن باشد، فریب می‌دهد. تا اینجا احتمال کلاهبرداری مشخص است. برای مثال اگر بی‌مقدمه کسی با شما تماس بگیرد و تقاضای پول کند، بعید است به حساب بانکی کسی که نمی‌شناسید، به آسانی پول واریز کنید. ولی اگر یکی از اعضای خانواده‌تان از طریق تماس تصویری همین درخواست را داشته باشد، چه؟ حتما نتیجه فرق خواهد کرد!

### راه‌حل مادر برابر قابلیت‌های جعل عمیق چیست؟

از قضا هوش مصنوعی، راه‌حلی برای این فناوری در آستین دارد. در حال حاضر با کمک هوش مصنوعی می‌توان ویدئوهای جعلی را تشخیص داد. ولی این الگوریتم‌های تشخیص، ضعفی جدی دارند؛ زیرا جعل عمیق برای افراد مشهور که ساعت‌ها فیلم رایگان از آنها در دسترس است بهترین عملکرد را دارد. شرکت‌های فناوری تلاش می‌کنند محتوای جعلی را در هر جا که منتشر می‌شود، تشخیص دهند. استراتژی‌های دیگری هم وجود دارد. برای مثال استفاده از واترمارک دیجیتال که البته چندان هم بی‌خطر نیست. اما یک سیستم بلاک‌چین می‌تواند ویدئوها، تصاویر و صداهای جعلی و هر دستکاری را تشخیص دهد و نسخه اصلی آنها را پیدا کند.

شد که نشان می‌داد در نشست خبری ترامپ، زمانی که کارمند کاخ سفید قصد داشته میکروفن را از آقای آکوستا بگیرد، وی رفتار تهاجمی داشته است. بعدا مشخص شد این فیلم درست در لحظه حساس سرعتش بیشتر شده و حرکت دست آکوستا تهاجمی جلوه داده شده است. پس از این اتفاق وی دوباره به کارش بازگشت. چه با جعل عمیق و چه با جعل کم‌عمق این دردرسرها روزبه‌روز بیشتر می‌شود و این فناوری نه‌تنها از بین نمی‌رود، بلکه کم‌کم جهان اطراف‌مان را غیرواقعی‌تر می‌کند. 📍

### جعل عمیق چطور ساخته می‌شود؟

مدت‌هاست پژوهشگران دانشگاه‌ها و استودیوهای جلوه‌های ویژه مرزهای هر آنچه را که می‌توان با دستکاری فیلم‌ها و صداها انجام داد، جابه‌جا کرده‌اند. به‌طور کلی دو روش برای ساخت فیلم‌های جعل عمیق وجود دارد. در روش اول تنها چند قدم طول می‌کشد تا ویدئویی با تغییر چهره‌ها بسازید. فرض کنید چهره دو نفر الف و ب را می‌خواهید با هم جابه‌جا کنید. ابتدا هزاران عکس از صورت این دو نفر را انتخاب کنید. حالا تمام تصاویر چهره‌های الف و ب را می‌دهیم به الگوریتمی از هوش مصنوعی که رمزنگار (encoder) نامیده می‌شود. رمزنگار شباهت‌های بین دو چهره را پیدا می‌کند، آنها را یاد می‌گیرد و بعد آنها را کدگذاری می‌کند. در قدم دوم الگوریتم هوش مصنوعی دیگری که رمزگشا (decoder) نامیده می‌شود، قرار است تصاویر کدشده را بازسازی کند. اما چون چهره دو نفر با هم تفاوت دارد، برای هر چهره رمزگشای مجزایی را باید تعریف کرد. رمزگشای اول تصویر چهره نفر الف و رمزگشای دوم تصویر نفر ب را بازسازی می‌کند. حالا در یک قدمی جابه‌جایی تصاویر هستیم. کافی است تصویر کدگذاری‌شده نفر الف را به‌عنوان ورودی به رمزگشای دوم بدهیم. رمزگشای دوم چهره نفر ب را با حالت و موقعیت چهره نفر الف بازسازی می‌کند. برای ساخت یک ویدئوی باورپذیر هم کافی است این‌کار را برای هر فریم تکرار کرد. روش دوم شبکه‌های مولد تخصصی (Generative Adversarial Network) یا گَن (GAN) نام دارد. در این روش دو الگوریتم هوش مصنوعی در برابر یکدیگر قرار می‌گیرند. الگوریتم اول که مولد (generator) نام دارد، داده‌های تصادفی را به تصویر تبدیل می‌کند. سپس تصویر ساختگی به زنجیره‌ای از تصاویر واقعی (مثل تصاویر افراد معروف) اضافه می‌شود و به‌عنوان ورودی به الگوریتم دوم که متمایزگر (discriminator) است، منتقل می‌شود. الگوریتم دوم کار ارزیابی داده‌های ورودی و تشخیص واقعی یا جعلی بودن تصاویر را برعهده دارد. هر بار که متمایزگر تشخیص درستی از جعلی‌بودن تصویر داشته باشد به مولد بازخورد می‌دهد. مولد هم بر اساس بازخورها، خطاهایش را تصحیح و جعل جدیدی می‌سازد. این فرآیند بی‌شمار مرتبه تکرار می‌شود تا عملکرد مولد و متمایزگر بهبود یابد تا جایی که مولد، چهره‌هایی کاملا واقعی از افراد معروفی می‌سازد که اصلا وجود خارجی ندارند.



### آیا جعل عمیق همیشه مخرب است؟

خیر! اتفاق بسیار سرگرم‌کننده و مفید می‌تواند باشد. برای مثال در جعل عمیق صوتی، می‌توان صدای افرادی را برگرداند که به‌دلیل بیماری صدای خود را از دست داده‌اند. ویدئوهای جعل عمیق به گالری‌ها و موزه‌ها روح تازه‌ای می‌بخشند. موزه سالوادور دالی در فلوریدا از نقاش سوررئالیست خود ویدئوی جعل عمیقی ساخته است که آثار خود را به بازدیدکنندگان معرفی و با آنها عکس سلفی می‌گیرد. در صنعت سرگرمی از این فناوری برای دوبله فیلم‌ها هم استفاده می‌شود. حتی این فناوری برای زنده کردن بازیگرانی که در دنیا رفته‌اند هم پیشنهاد می‌شود.

### ماجرای محتواهای جعل کم‌عمق از چه قرار است؟

فیلم‌های جعل کم‌عمق (shallow fakes) در بستری متفاوت ارائه می‌شوند و ابزارهای ویرایش ساده‌ای دارند. در این ویدئوها برای فریب مخاطب، سرعت پخش قسمتی از فیلم آهسته یا سریع می‌شود تا برداشت متفاوتی از فیلم را القا کند. گرچه برخی از این ویدئوها ناشیانه ساخته می‌شوند ولی تاثیر چشمگیری دارند. جیم آکوستا، خبرنگار سی‌ان‌ان مجوز ورودش به کاخ سفید پس از تنش لفظی با دونالد ترامپ لغو شد. پس از آن فیلم جعل کم‌عمقی منتشر

## گوگل هشدار مخصوص ناشنوایان را ارائه کرد

گوگل برای کاربران ناشناو ویژگی جدیدی در اندروید اضافه کرده‌که درصورت بازماندن شیرآب، پارس کردن سگ یا به‌صدا درآمدن زنگ هشدار آتش‌سوزی، آنها را مطلع کند. کاربران با اظهارهای صوتی و دیداری که روی نمایشگر ظاهر می‌شود، لرزش گوشی یا روشن شدن فلش دوربین چنین پیام هشداری را دریافت می‌کنند. / مهر

📍 در این روزهای داغ کارزار انتخابات آمریکا شما هم این فیلم

را دیده‌اید که بارک اوباما، رئیس جمهور سابق آمریکا، دونالد ترامپ را «حمقی به‌تمام معنا» خطاب می‌کند؟ یاقلمی که مارک زاکربِrg، صاحب شبکه اجتماعی فیسبوک، ادعا می‌کند کنترل کاملی روی اطلاعات دزدیده‌شده میلیون‌ها کاربر دارد؟ یاقلمی که‌شخصیت‌های بزرگ ومبارز تاریخ کشورمان‌ا کمیرزاچک‌خان جنگلی و ستارخان گرفته‌تا شهید همت وشهید چمران، سرود «ایران من» از همایون شجریان را می‌خوانند؟ اگر پاسخ شما به یکی از این سوال‌ها مثبت است، باید بگویم آنچه شما دیده‌اید فیلمی بوده‌که با فناوری جعل عمیق (DeepFake) ساخته‌شده است! فناوری جعل عمیق درواقع باکمک شکلی از فناوری هوش مصنوعی که یادگیری عمیق (Deep Learning) نامیده می‌شود، تصاویر یا فیلم‌هایی از اتفاقات غیرواقعی می‌سازد. برای همین آن را جعل عمیق می‌نامند. این فناوری نوبه افرادی که در زمینه هوش مصنوعی تخصصی ندارند، اجازه می‌دهد با داشتن تعداد زیادی عکس، یک ویدئوی جعلی بسازند. ساخت این فیلم‌های جعلی به خصوص در دنیای چهره‌های مشهور با سرعت بیشتری گسترش پیدا کرده است. اگر دوست دارید خودتان جای ستاره فیلم مورد علاقه‌تان بازی کنید، یا حرف‌های مورد نظر خودتان را از زبان فرد دیگری بگویید، فناوری جعل عمیق یاریگر شماست! در ادامه به ۱۰ سوال مهمی که معمولا در مورد جعل عمیق پرسیده می‌شود پاسخ می‌دهیم.

منبع: the Guardian

### آیا جعل عمیق فقط در مورد ویدئوهاست؟

خیر. فناوری جعل عمیق می‌تواند از صفر، تصاویری کاملا ساختگی اما باورپذیر بسازد. برای مثال پروفایل توئیتری و لینک‌داین کاربری با نام Maisy Kinsley که خود را خبرنگار ارشد رسانه بلومبرگ (Bloomberg) معرفی کرده است، وجود خارجی ندارد و یک پروفایل جعل عمیق است. همین‌طور حساب کاری Katie Jones که ادعا می‌کند در مرکز مطالعات راهبردی و بین‌المللی کار می‌کند نیز یک پروفایل جعل عمیق است که احتمالا برای عملیات جاسوسی ساخته شده است. حتی جعل عمیق در قالب صوتی نیز می‌تواند باشد، یعنی یک صدای شبیه‌سازی‌شده از اشخاص معروف ساخته شود. فروردین گذشته شرکتی بریتانیایی در حوزه انرژی یک تماس تلفنی از سوی شرکت مادر خود در آلمان دریافت می‌کند. در این تلفن از او خواسته می‌شود مبلغی نزدیک به ۲۰۰ هزار دلار را به حساب بانکی در مجارستان واریز کند. اما در واقعیت آن سوی تلفن کلاهبرداری نه‌نشسته بودند که صدای مدیرعامل شرکت آلمانی را تقلید کرده بودند. شرکت بیمه معتقد است صدا جعل عمیق بوده است، اما هنوز شواهد کافی در دست ندارد. گفته می‌شود کلاهبرداران از پیام‌های صوتی ضبط شده در واتس‌اپ استفاده کرده بودند.

### چه‌کسی جعل عمیق رامی‌سازد؟

همه! از پژوهشگران دانشگاهی و صنعتی گرفته‌تا افراد غیرحرفه‌ای که از روی علاقه این کار را دنبال می‌کنند. سیاستپون نیز ممکن است به‌عنوان قسمتی از استراتژی‌های آنلاین خود برای بی‌اعتبارکردن و بر هم زدن انسجام گروه‌های رقیب افراطی یا برقراری تماس با فردی خاص در این فناوری شُرک بکنند.

### چه‌نوع فناوری‌ای برای جعل عمیق نیاز است؟

اگر تا اینجا به فکر ساخت تصویر، ویدئو یا صدایی با فناوری جعل عمیق افتاده‌اید، بد نیست بدانید ساخت ویدئو، صدا یا عکسی در قالب جعل عمیق باکیفیت، آن هم با رایانه‌های معمولی کار سختی است. بیشتر این فیلم‌ها با رایانه‌های رده بالا با کارت گرافیک قدرتمند و از آن بهتر با قدرت محاسبه در فضای ابری ساخته می‌شود. زمان پردازش نیز از هفته‌ها و روزها به چند ساعت کاهش می‌یابد. همین‌طور سازندگان به مهارت بالایی در از بین بردن لرزش تصاویر و دیگر عیب‌های بصری در ویدئوها نیاز دارند. ولی ناامید نشوید، امروزه شرکت‌های زیادی ابزار و نرم‌افزارهایی را برای ساخت جعل عمیق در اختیارمان قرار می‌دهند و می‌توانیم چهره خود را جایگزین بازیگرهای بعضی از برنامه‌های تلویزیونی کنیم.

### چگونه جعل عمیق را تشخیص دهیم؟

به‌سختی! با پیشرفت فناوری این کار سخت‌تر هم می‌شود. سال ۹۷ بود که پژوهشگران دریافتند چهره‌هایی که با جعل عمیق ساخته شده‌اند، پلک نمی‌زنند. اما این کشف، کاربردی در مورد تصاویر جعل عمیق ندارد. چون همیشه افراد با چشم باز عکس می‌گیرند. ولی درمورد ویدئوها راه حلی جادویی به نظر می‌رسید. اما با انتشار این یافته، بلافاصله جعل عمیق‌هایی ساخته شد که در آنها پلک‌زدن هم وجود داشت. این طبیعت بازی است. به محض پیداشدن یک ضعف، آن را برطرف می‌کنند. تشخیص جعل عمیق‌های با کیفیت پایین ساده‌تر است. ممکن است حرکت لب‌ها همگام نشده یا رنگ پوست ناهمگون باشد. همین‌طور صورت که جابه‌جا می‌شود و لرزش تصویر وجود داشته باشد. به‌ویژه جزئیات ریز مثل موها در جعل عمیق معمولا با کیفیت ساخته نمی‌شود. جواهرات، دندان‌ها، روشنایی نامناسب محیط و بازتاب نور در عنیه چشم نیز می‌تواند سرنخی در این تشخیص باشد. دولت‌ها، دانشگاه‌ها و شرکت‌های فناوری همه به دنبال توانایی تشخیص جعل عمیق هستند. اولین مسابقه تشخیص جعل عمیق با حمایت شرکت‌هایی مثل مایکروسافت، فیسبوک و آمازون در سراسر جهان در حال برگزاری است. با نزدیک شدن به انتخابات آمریکا، شبکه‌های مجازی، ویدئوهای جعل عمیقی را حذف می‌کنند که حاوی اطلاعات نادرست باشند. اما این سیاست شامل ویدئوهای جعل کم عمق (shallow fakes) نمی‌شود.