في معركة الذكاء الصناعي، يستعد الباحثون للموجة القادمة من الدعاية المزيفة



حقوق الصورة: Pixabay/CC0 Public Domain.

تلقّى محقق صحفي مقطع فيديو من مجهول يظهر فيه مرشّح لمنصب الرئيس يعترف بنشاط غير قانوني، لكن هل هذا الفيديو حقيقي؟ إذا كان الأمر كذلك، فسيكون خبرًا كبيرًا، ويمكن أن يقلب الانتخابات القادمة تمامًا، لكنّ الصحفي يدير الفيديو من خلال أداة متخصصة تخبره أنّ الفيديو ليس كما يبدو في الواقع، إنه فيديو مزيف صُنِع باستخدام الذكاء الصناعي مع التعلّم العميق، وهو ما يعرف بالتزييف العميق أو (**deepfake**).

قد يتمكّن الصحفيون في جميع أنحاء العالم قريبًا من استخدام أداة كهذه. في غضون سنوات قليلة يمكن للجميع استخدام أداة مثل هذه

لاستئصال المحتوى المزيف في وسائل التواصل الاجتماعية الخاصة بهم.
يمكننا أن نرى مستقبلًا لهذه الأدوات كأداة للصحفيين من أجل اكتشاف التزييف العميق، ومع ذلك لن تحل جميع مشاكلنا، وستكون مجرد جزء واحد من ترسانة الحرب على المعلومات المضللة.

مشكلة التزييف العميق

يعرف معظم النّاس أنه لا يمكنك تصديق كل ما تراه، فعلى مدى العقدين الماضيين اعتاد مستهلكو الأخبار على رؤية صور متلاعب بها باستخدام برامج تحرير الصور. على الرغم من ذلك، تُعدّ مقاطع الفيديو قصّة أخرى. يمكن لمخرجي هوليوود إنفاق ملايين الدولارات على المؤثرات الخاصة لعمل مشهد واقعي، ولكن باستخدام تقنية التزييف العميق يمكن للهواة الذين يمتلكون بضعة آلاف من الدولارات من أجهزة الحاسوب، ومع قضاء بضعة أسابيع في العمل عليها أن يصنعوا شيئًا ما يُعدّ واقعيًا.

تتيح تقنية (**Deepfakes**) وضع الأشخاص في مشاهد أفلام لم يكونوا فيها من قبل ـ فكّر في (**Tom Cruise**) يلعب شخصية **Iron Man**، ما يجعل مقاطع الفيديو مسليّة. لسوء الحظ، فإنه يجعل من الممكن أيضًا إنشاء مواد إباحية دون موافقة الأشخاص الذين يُصوَّرون. حتى الآن، أكبر ضحايا إساءة استخدام تقنية التزييف العميق هم النساء.

يمكن أيضًا استخدام تقنية (**Deepfakes**) لإنشاء مقاطع فيديو لقادة سياسيين يقولون أشياء لم يقولوها مطلقًا. أصدر الحزب الاشتراكي البلجيكي مقطع فيديو منخفض الجودة غير مزيف، ولكنه مصنَّع للرئيس ترامب وهو يهين بلجيكا، والذي حصل على رد فعل كاف لإظهار المخاطر المحتملة للتزييف العميق عالي الجودة.

ربما يكون الأمر الأكثر رعبًا على الإطلاق، إذ يمكن استخدامها لإثارة الشّك حول محتوى مقاطع الفيديو الحقيقية من خلال اقتراح أنها قد تكون مزيفة.

بالنظر إلى هذه المخاطر، سيكون من المفيد للغاية أن نكون قادرين على اكتشاف التزييف العميق وتصنيفه بوضوح. سيضمن هذا أن مقاطع الفيديو المزيفة لا تخدع الجمهور، وأن مقاطع الفيديو الحقيقية يمكن تلقيها على أنها أصلية.

اكتشاف التزييف

بدأ اكتشاف التزييف العميق كمجال بحثي منذ ما يزيد قليلًا عن ثلاث سنوات. ركّز العمل المبكر على اكتشاف المشكلات المرئية في مقاطع الفيديو مثل التزييف العميق الذي لا يرمش. ومع ذلك، مع مرور الوقت أصبحت المنتجات المقلّدة أفضل في محاكاة مقاطع الفيديو الحقيقية، وأصبح من الصعب اكتشافها لكل من الأشخاص وأدوات الكشف.

هناك فئتان رئيسيتان لأبحاث الكشف عن التزييف العميق. الأول يتضمّن النظر إلى سلوك الأشخاص في مقاطع الفيديو. لنفترض أن لديك الكثير من مقاطع الفيديو لشخص مشهور، مثل الرئيس أوباما. يمكن للذكاء الصناعي استخدام هذا الفيديو لمعرفة أنماطه من خلال إيماءات يده إلى توقفاته في الكلام. يمكنه بعد ذلك مشاهدة صورة مزيفة له وملاحظة عدم تطابقها مع تلك الأنماط. يتمتع هذا النهج بميزة إمكانية العمل حتى لو كانت جودة الفيديو نفسها مثالية بشكل أساسي.

ركّز باحثون آخرون ومن بينهم فريقنا على الاختلافات التي قارنتها جميع تقنيات التزييف العميق بمقاطع الفيديو الحقيقية. غالبًا ما تُنتَج مقاطع الفيديو المزيفة عن طريق دمج الإطارات التي تُنتَج بشكل فردي لتكوين مقاطع الفيديو. مع أخذ ذلك في الاعتبار تستخرج أساليب فريق البحث البيانات الأساسية من الوجوه في الإطارات الفردية للفيديو ثم تتبعها من خلال مجموعات من الإطارات المتزامنة. ما يسمح لنا باكتشاف التناقضات في تدفق المعلومات من إطار إلى آخر، ويقوم فريق البحث باستخدام نهجًا مشابهًا لنظام اكتشاف الصوت

المزيف أيضًا.

يصعب على الناس رؤية هذه التفاصيل الدقيقة، لكنها تُظهر كيف أن التزييف العميق ليس مثاليًا. يمكن أن تعمل أجهزة الكشف مثل هذه مع أي شخص، وليس فقط عدد قليل من قادة العالم. في النهاية، قد تكون هناك حاجة لكلا النوعين من أجهزة الكشف عن التزييف العميق.

تعمل أنظمة الكشف الحديثة بشكل جيد للغاية على مقاطع الفيديو التي جُمعت خصيصًا لتقييم الأدوات. لسوء الحظ، حتى أفضل النماذج تعمل بشكل سيئ على مقاطع الفيديو الموجودة على الإنترنت. الخطوة التالية الرئيسية هي تحسين هذه الأدوات لتكون أكثر قوة وفائدة.

مَن يجب أن يستخدم كاشفات التزييف العميق؟
من الناحية المثالية، يجب أن تكون أداة التحقق من التزييف العميق متاحةً للجميع. ومع ذلك، فإن هذه التكنولوجيا في المراحل الأولى من التطوير، ولذلك يحتاج الباحثون إلى تحسين الأدوات وحمايتها من المتسللين قبل إطلاقها على نطاق واسع.

ولكن في الوقت نفسه، فإن أدوات التزييف العميق متاحة لأي شخص يريد خداع الجمهور، إذًا فالجلوس على الحياد ليس خيارًا. بالنسبة لفريق البحث كان التوازن الصحيح هو العمل مع الصحفيين، لأنهم يمثلون خط الدفاع الأول ضد انتشار المعلومات المضللة.

قبل نشر القصص يحتاج الصّحفيون إلى التحقق من المعلومات، وفي حين لديهم بالفعل طرق مجربة وحقيقية، مثل التحقق من المصادر والحصول على أكثر من شخص للتحقق من الحقائق الأساسية، فمن خلال وضع أداة الكشف عن التزييف في أيديهم، نقدم لهم المزيد من المعلومات، ونعلم أنهم لن يعتمدوا على التكنولوجيا وحدها، نظرًا لإمكانية ارتكابها أخطاء.

هل تستطيع أجهزة الكشف الفوز في السباق؟
من المشجع أن نرى فرقًا من **Facebook** و **Microsoft** تستثمر في تكنولوجيا فهم التزييف العميق واكتشافه. يحتاج هذا المجال إلى مزيد من البحث لمواكبة سرعة التقدم في تقنية التزييف العميق.

يحتاج الصحفيون ومنصّات التواصل الاجتماعي أيضًا إلى معرفة أفضل السبل لتحذير الناس من التزييف العميق عند اكتشافهم له. أظهرت الأبحاث أن الناس يتذكرون الكذبة، لكن ليس حقيقة أنها كانت كذبة، فهل ينطبق الأمر نفسه على مقاطع الفيديو المزيفة؟ وهل يكون وضع كلمة "**Deepfake**" في العنوان كافيًا لمواجهة بعض أنواع المعلومات المضللة.

تقنية التزييف العميق هنا لتبقى، وستكون إدارة المعلومات المضللة وحماية الجمهور أكثر صعوبةً من أي وقت مضى حيث تزداد قوة الذكاء الصناعي. نحن جزء من مجتمع بحثي متنامٍ يتعامل مع هذا التهديد، والذي يكون اكتشاف التزييف فيه مجرد الخطوة الأولى.

- التاريخ: 2021-08-23
- التصنيف: الذكاء الاصطناعي

#الذكاء الصنعي #الذكاء الاصطناعي #التزييف العميق #الدعاية المزيفة

المصادر

- Tech Xplore

المساهمون

- ترجمة
  - محمد السيد عبده
- مُراجعة
  - سارة صالح
- تحرير
  - رأفت فياض
- تصميم
  - Azmi Salem
- نشر
  - آلان حسن