المجلد 6، العـدد 23 ص 12 - 24 (2025)، Volume 6, Issue 23

تطبيقات و خوارزميات الذكاء الاصطناعي وجر ائم و انتهاكات التزوير والتزييف العميق

[1] د. محمد عثمان محمد قسم السيد ، [2] د. ياسر الملك أحمد سليمان*

[1]الجامعة التكنولوجية (السودان)، [2] الجامعة التكنولوجية (السودان)

Artificial intelligence applications and algorithms, crimes and violations of forgery and deep fakes

[1]Dr. Mohamed Osman Mohamed Gasm Elseid *, [2] Full Dr. YasserElmalik Ahmed Seleman

[1] https://orcid.org/0009-0006-4395-5001, [2] https://orcid.org/0009-0007-2052-0408

[1] University of Technology (Sudan)

[2] University of Technology (Sudan), dr.yaserking359@hotmail.com

تاريخ الاستلام: 22 / 04 /2025 تاريخ القبول: 23 / 05 / 2025 تاريخ النشر: 01 / 09 / 2025

الملخص:

تناول البحث العديد من الخدمات المفيدة لتطبيقات الذكاء الاصطناعي وتناول المشاكل والجرائم في الفترة الأخيرة والتي أصبحت جزء رئيسي في العديد من جرائم الاحتيال والتزييف للصور والمكالمات والفيديوهات بصورة أقرب للواقع الأصلي وهو ما يسمى بالتزييف العميق، يهدف البحث إلى تحليل الأسس التقنية التي تقوم عليها تقنية التزييف العميق، مع تسليط الضوء على تأثيراتها العميقة على صناعة الإعلام وثقة الجمهور في المعلومات، وكذلك يشرح البحث مشكلة تقنيات وخوارزميات الذكاء الاصطناعي والتزييف العميق لإنشاء مقاطع فيديو أو تسجيلات صوتية اثبتت قدرتها على التأثير في الرأي العام والسياسات من خلال إنشاء محتويات مفبركة تُستخدم لأغراض خبيثة، مثل التأثير في نتائج الانتخابات أو تشويه سمعة الشخصيات العامة.

اتبع الباحثون المنهج الوصفي في وصف المشكلة والمنهج التحليلي في تحليل مشكلة المشكلة الوصول لحلول من خلال امثلة لبرامج وتطبيقات. تم التوصل من خلال البحث لنتائج وتوصيات عملية في حلول مشاكل التزييف العميق والتزوير.

كلمات مفتاحية: تطبيقات الذكاء الاصطناعي.، الجرائم الإلكترونية.، التزييف العميق.، الجرائم السيبرانية.، تقنية المعلومات.

Abstract:

The research deals with a Despite the many benefits of AI applications, However, in recent years, it has turned to be a major tributary in the commission of many crimes, and the manufacture of the so-called "deep lie", which is a type of lie, that has the ability to produce still, moving, and speaking images that resemble the truth. And in light of the amazing progress witnessed in the world of artificial intelligence; It has become easy to fake realistic-looking videos and photos, in a process known as deep fake , The research explains the problem of artificial intelligence and deep fake technologies and algorismthms for creating videos or audio recordings that have proven their ability to influence public opinion and policies by creating fabricated content used for malicious purposes, such as influencing election results or defaming public figures.

The researchers followed the descriptive approach in describing the problem and the analytical approach in analyzing the problem to reach solutions through examples of programs and applications, Practical results and recommendations were reached in solving the problems of deep fake and forgery.

Keywords: Artificial intelligence applications; Cybercrimes; deep fake; cybercrime; information technology.

مقدمة:

شهد الذكاء الاصطناعي تطوّراً كبيراً في تقنياته وبشكل سريع، مع ظهور الذكاء التوليدي أصبحت محتويات التقنية تبدو وكأنها من صنع البشر وأضحت تقوم بعمل الإنسان في بعض الأحيان، ما يثير المخاوف من إساءة إستخدام الذكاء الاصطناعي لأغراض خبيثة مثل التضليل والاحتيال والخداع والتأثير على المجتمع. وفي السنوات الأخيرة بدأت ظهور تقنيات التزييف العميق التي يمكن من خلالها تعديل الصور والفيديوهات بشكل يجعل من الصعب التمييز بين المحتوى الأصلي والمعدّل وما يسمي بالتزييف العميق هو إحدى أبرز التقنيات التي تعتمد على الذكاء الاصطناعي لإنشاء أو تعديل الفيديوهات والصور بطريقة تجعلها تبدو حقيقية، تستخدم هذه التقنية بشكل رئيسي الشبكات العصبية التوليدية ومجموعه من الأدوات. أن تقنيات الأعمال المزيفة تكون متطورة ومعقدة للغاية وأصبحت متاحة بشكل متزايد، مما يجعل برامج الكشف عنها والقوانين الضابطة لها صعب ويحتاج الي توعية وتطوير تقنيات للحد من مثل هذه الجرائم والانتهاكات.

يعد الذكاء الاصطناعي بشكلٍ عام من الأدوات التي يمكن إساءة استخدامها، مما يؤدي إلى مشاكل كثيرة، مثل التحيز، وانتهاكات الخصوصية، ويؤدي ظهور تقنيات التزييف العميق إلى تضخيم هذه المخاطر، حيث تعتبر تقنيات التزييف العميق وسائط اصطناعية شديدة الواقعية تم إنشاؤها باستخدام تقنيات التعلم العميق، التي تتلاعب بوسائط الصوت أو الفيديو أو أي محتوى رقمي آخر، مما يجعل من الصعب التمييز بين المواد الأصلية والمزيفة.

1- مشكلة البحث:

تكمن مشكله البحث الأساسية في التحديات التي تواجه العالم وتتسبب في دمار ومشاكل لعديد من الدول والشعوب من خلال الاستخدام السلبي لتقنيات وخوارزميات الذكاء الاصطناعي فقد أصبح التزييف العميق أخطر أنواع هذه التقنيات التي تعتمد على خوارزميات التعلم العميق لإنشاء مقاطع فيديو أو تسجيلات صوتية تبدو وكأنها حقيقية و يمكن استخدامها لتقليد أصوات وأشكال الأشخاص بدقة شديدة، مما يجعل المحتوى المزيف صعب التمييز عن الواقع, تعتمد التقنية على تدريب الشبكات العصبية على كميات هائلة من البيانات التي تتضمن الأصوات والصور والفيديوهات للأشخاص المستهدفين تطرق الباحثون لمثال فيديوهات كانت سبب لتأجيج الصراع والحرب الحالية في السودان.

يتسبب التزييف في مجموعة من المشاكل يلخص الباحثون أهمها في النقاط التالية:

1- إستخدام التزييف لانتحال صوت مدير في إحدى الشركات أو البنوك، وتحويل أموال إلى حساب المهاجم، وهي مثال على الطريقة التي يمكن أن يستغل بها المهاجمون هذه التقنية للحصول على أموال أو معلومات حساسة.

2- إستُخدام فيديوهات مزيفة لإقناع الأفراد بالقيام بمعاملات احتيالية.

3- إستُخدام فيديوهات مزيفة لزعماء ورؤساء دول او شخصيات يمكن أن تكون للتأثير على الشعوب والدول وإثارة حرب ونزاعات لأهداف معينة.

2- تساؤلات البحث:

- ما هي الخوارزميات والتقنيات المستخدمة في اكتشاف التزييف العميق والتحليل لبيانات التعريف الخاصة بالملف وضمان عدم التعديل والتأكد من المصداقية؟
- كيف تتم الانتهاكات التزوير والتزييف العميق وهل هناك تأثيرات للتزييف العميق؟
- هل توجد تدابير تقنية وإجرائية لإيجاد حلول للحد من الانتهاكات؟
- هل تساهم التدابير التقنية في حماية الذكاء الاصطناعي؟

3- الهدف من البحث:

يهدف البحث للتعرف على جرائم وانتهاكات الذكاء الاصطناعي والطرق لمكافحة الجرائم والانتهاكات وتوضيح التزييف العميق والتقنيات والأدوات التي يمكن استخدامها للكشف عنه وتمكين مصادقة الوسائط الحقيقية وكيفية إستخدام التعلم الآلي كتقنية من تقنيات الذكاء الاصطناعي والخوارزميات الحديثة التي تهدف للكشف وتحديد الوسائط المزيفة دون الحاجة الي مقارنتها بالوسائط الأصلية غير المعدلة.

4- أهمية البحث:

تتمثل في مجموعة نقاط هامة ظهرت حديثاً وهي وانتهاكات الذكاء الاصطناعي من خلال التزوير والتزييف وانتحال الهوية ونشر المعلومات مضلله والتزوير لفيديوهات ومكالمات وتسجيلات تضر بالأفراد والمؤسسات والدول وشهدت الشركات والبنوك ووكالات الإعلام لمثل هذه الجرائم يتم توضيحها في البحث والسعي في معرفة الأسباب التي أدت لذلك والوقاية من الانتهاكات، ومثل هذه الجرائم، وضمان أمن البيانات والمعلومات وتفاديا لها في المستقبل للتأثير العالمي الكبير.

5- منهجية البحث:

اتبع الباحثون في منهجية البحث المنهج الوصفي والتحليلي المنهج الوصفي في الشرح والتوصيف للمشكلة ومن ثم التحليلي لشرح المشكلة والمساهمة في كيفية إيجاد طرق عديده تساعد في الحلول والتوصل لنتائج البحث الضرورية.

6- حدود البحث:

اقتصر البحث على التعرف لتطبيقات وخوارزميات الذكاء الاصطناعي وجرائم وانتهاكات التزوير والتزييف العميق وتأثيره على المؤسسات الحكومية الكبيرة في الدول المتقدمة والثغرات ونقاط الضعف وكيفية إجراء التدابير المناسبة.

حدود زمانية: أجريت الدراسة في بداية مارس2025.

حدود مكانية: اهتم البحث بالمؤسسات الحكومية والوزارات المهمة واهمها وزارة الاعلام.

خطة البحث:

إن متطلبات الدراسة العلمية وطبيعة الموضوع والغرض من البحث تجعل من المناسب أن نعالج هذا الموضوع من خلال مقدمة، ومحور تمهيدي ونظري، ومحور تطبيقي وعملي وخاتمة حيث يتناول المحور التمهيدي: مفهوم التزييف العميق، أشكال ومفهوم جرائم التزييف العميق، سبل مواجهة جرائم التزييف العميق.

المحور الأول: الجانب النظري للبحث:

1. مقدمة الذكاء الاصطناعي: [1]

الذكاء الاصطناعي تم استخدامه بشكل متزايد في عالم الجرائم الإلكترونية من قبل المهاجمين والأدوات والتقنيات التي تعتمد على الذكاء الاصطناعي توفر فرصًا لهجمات أكثر تعقيدًا وصعوبة في الاكتشاف مقارنة بالهجمات التقليدية كما يمكن إستخدام الذكاء الاصطناعي لتحليل الأنماط السلوكية، مما يساعد المهاجمين على معرفة أكثر النقاط ضعفًا في الأنظمة الأمنية" واستخدام تقنيات محاكاة أساليب تواصل محددة بناءً على تحليلات البيانات الشخصية للأفراد.

وباستخدام تقنيات التعلم العميق والشبكات العصبية، يمكن إنشاء مقاطع فيديو صوت تُحاكي شخصيات مشهورة أو حتى أفراد عاديين في مواقف لمتحدث في الواقع في عصرنا الرقمي الحالي أصبح الذكاء الاصطناعي (AI) أداة قوية تتسم بتعدد استخداماتها في مجالات عدة، بدءًا من تحسين الإنتاجية وزيادة الكفاءة وصولاً إلى تهديدات غير مرئية تزعزع الأمان الرقمي. ومن بين أبرز المجالات التي أظهر فيها الذكاء الاصطناعي تأثيره هو الجرائم الإلكترونية والتزييف العميق (Deepfake)، والتي باتت تهدد الأفراد والمؤسسات والدول.

2- **الذكاء الاصطناعي و الجرائم الإلكترونية:**[2]

أصبحت تقنيات و أدوات الذكاء الاصطناعي تؤثر بشكلٍ كبير على الاقتصاد والطب والإعلام وجميع النواحي الحياتية، و بشكلٍ عام يمكن إساءة إستخدام هذه الأدوات مما يؤدي إلى مشاكل كثيرة، مثل :التحيز، وانتهاكات الخصوصية، ويؤدي ظهور تقنيات التزييف العميق إلى تضخيم هذه المخاطر، حيث تعتبر تقنيات التزييف العميق وسائط اصطناعية شديدة الواقعية تم إنشاؤها باستخدام تقنيات التعلم العميق فمعالجة هذه القضايا أمر ضروري للحفاظ على سلامة المعلومات، وحماية سمعة الأفراد، وضمان السلامة العامة، إذ تؤدي صعوبة اكتشاف وتحديد أساليب التزييف العميق وتقنياته نظراً إلى أن تقنيات التزييف العميق أصبحت أكثر تقدماً ويمكن الوصول إليها، فقد تصاعدت المخاطر المرتبطة بها عالمياً, من خلال البحث يوضح الباحثون كيف يستخدم الذكاء الاصطناعي في ارتكاب الجرائم الإلكترونية، وكذلك تأثيره على إنتاج محتوى زائف وتوليد فيديوهات مزوره ومزيفة تشبه الواقع الحقيقي.

واستعراض سلسلة من الخطوات الآلية التي تساعد في تقديم التعليمات البرمجية بسرعة أكبر وأكثر أمان للتعرف على التزييف العميق وكيفية الاكتشاف وإستراتيجيات التخفيف من المخاطر لكل مرحلة.

للتخفيف من المخاطر المرتبطة بالتزييف العميق، يجب على مؤسسات الدولة تنفيذ أمثلة نموذجية حول كيفية استفادة هذه القطاعات من التطبيقات المبتكرة والقيمة للتزييف العميق تستعرض في شكل مراحل تم التفصيل لها من خلال الباحثون كالاتي:

- تقنيات التزييف ويشتمل على كل الانواع (صور، صوت، فيديو).
- إستخدام أدوات الذكاء الاصطناعي والتحقق من التزييف.
- جانب تطبيقي يوضح كيفية الاستخدام.

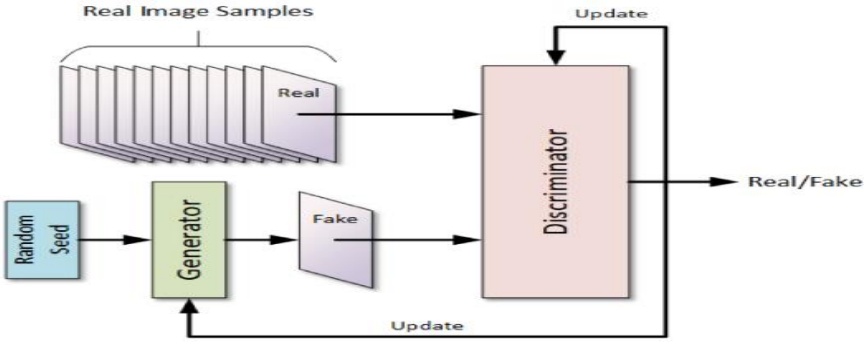
- تقنيات التزييف الصوتي العميق: [3]

إنشاء التزييفات الصوتية العميقة باستخدام شبكات الخصومة التوليدية (GANs) وخوارزميات التعلم العميق التي يمكنها تحليل وتكرار الفروق الدقيقة في أنماط الكلام البشري. ومن خلال تدريب هذه النماذج على مجموعات بيانات كبيرة من العينات الصوتية، يمكن لأنظمة الذكاء الاصطناعي تجميع تسجيلات صوتية واقعية للغاية تحاكي صوت فرد معين, مع التقدم في معالجة اللغة الطبيعية وتركيب الكلام، أصبح من الصعب بشكل متزايد التمييز بين المحتوى الصوتي الأصلي والمحتوى الصوتي الذي تم التلاعب به , يشكل هذا تحديًا كبيرًا لكشف ومكافحة انتشار التزييف الصوتي العميق في المشهد الرقمي. ، إنَّ انتشار الملفات الصوتية المزيفة يثير مخاوف جدية بشأن إدارة السمعة والخصوصية والأمن ، يمكن استهداف الزعماء والرؤساء بتصريح مزيف يؤدي إلى ردة فعل ، قد يقع المشاهير والشخصيات العامة ضحية التزييف الصوتي العميق او إن استغلال التزييف الصوتي العميق لأغراض الابتزاز أو الدعاية يؤكد بشكل أكبر على الحاجة لحماية المجتمع من التزييف الرقمي.

(أ) - توليد الصور والفيديوهات باستخدام الذكاء الاصطناعي(AI-Generated Content) : تمّ تطوير نماذج ذكاء اصطناعي قادرة على إنشاء محتوى مرئي بالكامل هذه النماذج تعتمد على تعلّم الأنماط البصرية من مجموعات ضخمة من البيانات، وتمكّنها من توليد صور وفيديوهات واقعية بناءً على أوصاف نصيّة أو معطيات معيّنة و نماذج (Generative Models)مثل GANsو VAEs تستخدم هذه النماذج في توليد محتوى مرئي جديد، مثل صور لأشخاص أو أماكن غير موجودة في الواقع على سبيل المثال، يمكن للنماذج مثل StyleGAN إنشاء صور لأشخاص خياليّين تبدو حقيقية جداً رغم أنها غير موجودة في الواقع.

(ب)- تحسين الجودة والتفاصيل: يمكن استخدام الذكاء الاصطناعي لتحسين جودة الفيديوهات أو الصور المعدّلة، مما يجعلها تبدو أكثر احترافية وأصيلة، حتى لو كانت قد خضعت للتعديل.

(ج)- يمكن استبدال وجه شخص في فيديو بآخر باستخدام تقنيات التزييف العميق، كما يحدث في التطبيقات مثل "DeepFaceLab"أو."FaceSwap" تعديل تعابير الوجه: يمكن تعديل تعابير الوجه لجعل الشخص يظهر وكأنه يقول شيئاً لم يقله في الواقع، مما يتيح نشر معلومات مضلّلة أو التشهير. إعادة تشكيل الصوت: يمكن أيضاً استخدام الذكاء الاصطناعي لتقليد الأصوات البشرية، مما يجعل التزييف العميق أكثر إقناعاً.



الشكل (1) يوضح التزييف العميق للصور- (ايهاب خليفة 2019)

تُعتبر الخلايا العصبية بمثابة وحدات برمجية تقوم بوظيفة استقبال وإرسال البيانات التي يتم تغذية النظام بها, ومن خلال وضع هذه الخلايا في صورة متضادة مع بعضها يساعدها ذلك في توليد نماذج إحصائية ومعلوماتية أكثر مكّنت من رسم صور أكثر كفاءة ودقة, ويحدث ذلك من خلال وضع خلية عصبية في مواجهة خلية عصبية أخرى، أن الخليتين تم تدريبهم على نفس قواعد البيانات التي تم تغذية النظام بها, تقوم الأولى بمحاولة ابتكار وتصميم الصورة، وتقوم الثانية بدور المحقق أو المميز للاختلاف في الصورة، وذلك من خلال اكتشاف نقاط الخلل داخل الصورة, ويتم تسمية الخلية الأولى باسم المولد generator، والثانية باسم المميز discriminator. وعند قيام الخلية الثانية باكتشاف الخلل تقوم الخلية الأولى تصحيحه حتى تعجز الخلية الثانية عن اكتشافه، ومن ثم يخلق النظام الشكل النهائي للصورة التي يصعب اكتشاف التزوير والتزييف [4].

اهتمام البحث بمشكلة جرائم الذكاء الاصطناعي والتزييف العميق والتعرف على الكيفية التي تتم وطرق التخفيف والحد من الانتهاكات، من خلال خطة علمية وعملية تشرح المشاكل الحقيقية و الواقعية ومن ثم توضيح استغلال الذكاء الاصطناعي والتقنيات في هذه الجرائم التي يشكلها التزييف العميق ويتمثل أبرزها في التحايل على الشخصيات العامة، حيث يمكن للذكاء الاصطناعي أن يستخدم لإنشاء مقاطع فيديو أو تصريحات مزيفه لرؤساء دول، سياسيين، أو شخصيات عامة، مما يؤثر على سمعتهم ويزعزع الثقة العامة إعداد إستراتيجيات دقيقة وتفصيلية لجميع جوانب المخاطر الناجمة عن استخدامات الذكاء الاصطناعي، خاصة ما يتعلق بالتزييف والتلاعب والسرقة والهجمات الإلكترونية وحماية البيانات[5].

يذكر الباحثون أمثلة للتزييف العميق [1]:

أ- الشكوك حول فيديوهات لقائد مليشيات عسكرية في السودان كانت سبب الحرب الأخيرة وأتضح وفاته وتتواصل ظهور الفيديوهات وربوت لإثاره ومواصلة الحرب وهي ستكون بمثابة جريمة العصر التكنولوجية.

ب- تزييف فيديو يظهر فيها مارك زوكربيرغ، المؤسس والمدير التنفيذي لموقع التواصل الاجتماعي (Facebook)ومدير شركة " (Meta) "وهو يعترف بتآمره في مشاركة بيانات المستخدمين.

ج- فيديو لرئيس الولايات المتحدة السابق باراك أوباما يتحدث عن رئيس أخر بصورة لا تليق بدولة عُظمى، وأتضح أخيرا أن الفيديو كان مزيف وأستخدم للدعاية الانتخابية [6].

د- في منطقة آسيوية، تم خداع موظف في شركة متعددة الجنسيات لتحويل مبلغ كبير من المال إلى المحتالين من خلال تقنية التزييف العميق لانتحال شخصية أحد كبار المسؤولين التنفيذيين خلال مكالمة عبر الفيديو.

في الانتخابات الأمريكية تم إستخدام تقنيات التزييف العميق لإنشاء مقاطع فيديو مزيفة للمرشحين، ونشر معلومات مضللة بهدف تغيير تصورات واصوات الناخبين من خلال مقاطع الفيديو المزيفة أحد المرشحين البارزين وهو يُدلي بتصريحات مثيرة للجدل، مما أدى إلى انخفاض ملحوظ في شعبيته ومستوى دعمه، على الرغم من الجهود اللاحقة لدحض الفيديو وبيان زيفه.

- **إستخدام أدوات الذكاء الاصطناعي والتحقق من التزييف**[7]:

في العصر الرقمي الحديث ظهرت التزييفات العميقة باعتبارها تهديدًا كبيرًا لأصالة المحتوى الحقيقي، يمكن لمقاطع الفيديو المتطورة التي تم إنشاؤها بواسطة الذكاء الاصطناعي أن تحاكي الأشخاص الحقيقيين بشكل مقنع، ما يزيد من صعوبة التمييز بين الحقيقة والخيال، إستخدام أدوات الذكاء الاصطناعي المتقدمة لتحليل مقاطع الفيديو والصور بحثاً عن علامات التزييف، بالإضافة إلى ذلك فحص البيانات الوصفية للمحتوى الرقمي التي توفر تفاصيل حول تواريخ الإنشاء ومحفوظات التحرير والبرامج المستخدمة، مما يساعد في التحقق مما إذا كان المحتوى قد تم تغييره والتعديل وذلك يكون بفهم العناصر الرئيسية وعمليات التحقق.

- **العناصر الرئيسية للتوصل للحلول مثل الجوانب التالية** (8) :

1-فهم تقنية التزييف العميق :تقديم نظرة شاملة حول كيفية إنشاء حالات التزييف العميق، بما في ذلك خوارزميات وتقنيات الذكاء الاصطناعي الأساسية المعنية.

2- آليات الكشف :تعليم الأساليب المتقدمة لتحديد التزييف العميق، مثل :تحليل التناقضات في الفيديو والصوت، باستخدام أدوات الكشف القائمة على الذكاء الاصطناعي، والتعرف على علامات الوسائط الاصطناعية.

3- الاعتبارات الأخلاقية والنظامية :استكشاف الآثار الأخلاقية والأطر النظامية المتعلقة باستخدام التزييف العميق لضمان ممارسات مسؤولة وممتثلة للقانون.(9)

4- التدريب العملي :تقديم جلسات عملية حيث يمكن للمستخدمين النهائيين العمل مع أدوات الكشف ومجموعات البيانات لاكتساب خبرة عملية في تحديد التهديدات العميقة والتخفيف منها ولضمان بقاء المستخدمين النهائيين مطلعين على أحدث التطورات وأفضل الممارسات .التحقق تتم من خلال إتباع خطوات في عملية التحقق من خلالها يتم تحديد الآلية المتبعة في خطوات، وهي:

- **التحقق اليدوي والاحترافي:**

خدمات التحقق من الحقائق :إستخدام الخدمات الاحترافية لتدقيق الحقائق للتحقق من صحة المحتوى المشبوه ويمكن من خلال تكوين فريق إشراك خبراء الذكاء الاصطناعي والمبرمجين وخبراء الطب الشرعي الرقمي لفحص المحتوى يدوياً بحثاً عن علامات بالتزييف العميق، مثل (ملامح الوجه غير المنتظمة، والحركات غير الطبيعية، والتناقضات بين الصوت والمرئيات).

- **التحقق الآلي والمحوسب:**

إستخدام التقنيات والخوارزميات الحديثة وبعض البرامج لإجراء عمليات التدقيق للتأكد من الحقائق وهو جانب ومحور تطبيقي للبحث.

المحور الثاني

محور تطبيقي

في هذا المحور يتناول الباحثون أهم التقنيات والتطبيقات التي تساهم في اكتشاف التزييف العميق وكيفية إستخدام هذه التطبيقات في اكتشاف التزييف العميق والتزوير وتساهم بقدر كبير في مواجهه الجرائم والانتهاكات والحد من انتشار هذه الظاهرة، سيتم مناقشة الأدوات الحديثة وكيفية استخدامها.

مع تقدم التكنولوجيا الكامنة وراء التزييف العميق، تقدمت أيضًا الأدوات والتقنيات المصممة لاكتشافها, يناقش الباحثون في هذا المحور أفضل أدوات وتقنيات للكشف عن التزييف العميق المتاحة وسيتم مناقشة الأدوات من خلال البحث وأن أهم هذه التقنيات والأدوات الحديثة هي (10):

1- مدافع الو اقع Reality Defender:

تتكيف Reality Defender بشكل مستمر مع تقنيات Deepfake المتطورة، وتحافظ على دفاع قوي ضد التهديدات في وسائل الإعلام والتمويل والحكومة.

المميزات الرئيسية للمدافع عن الو اقع:

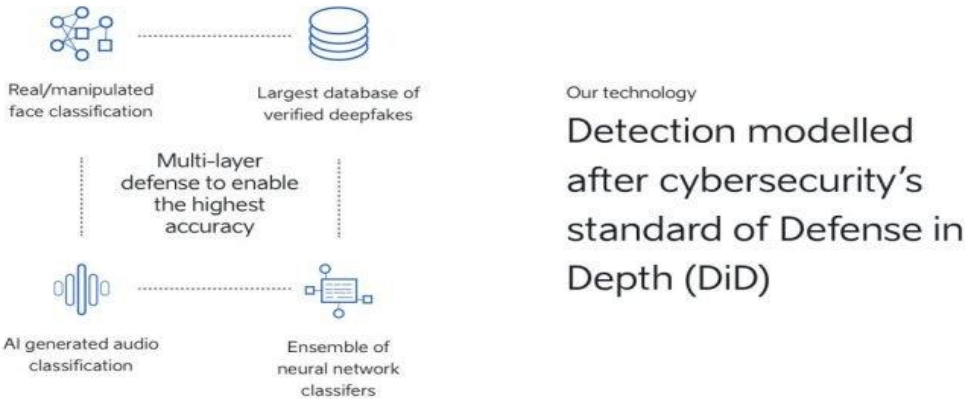
- يكتشف تطبيق Reality Defender عمليات التزييف العميق في الصور ومقاطع الفيديو والصوت والنصوص للمؤسسات والحكومات.
- يوفر اكتشافا في الوقت الفعلي وخاليًا من العلامات المائية للتحقق السريع من المحتوى.
- يمكن الوصول إليها عبر تطبيق الويب أو واجهة برمجة التطبيقات القابلة للتطوير لتحقيق التكامل المرن.
- يقدم رؤى واضحة للتلاعب لتوجيه إجراءات الاستجابة.
- يتم تحديثه باستمرار لمحاربة تهديدات الذكاء الاصطناعي المتطورة.

2 -حارس Sentinel :

تستخدم خوارزميات الذكاء الاصطناعي المتقدمة لتحليل الوسائط التي تم تحميلها وتحديد ما إذا كان قد تم التلاعب بها, يقدم النظام تقريرًا مفصلاً عن نتائجه ، بما في ذلك تصور لمناطق وسائل الإعلام التي تم تغييرها, تم تصميم تقنية اكتشاف التزييف العميق من Sentinel لحماية سلامة الوسائط الرقمية، تساعد الحكومات ووكالات الدفاع والمؤسسات على وقف تهديد التزييف العميق, تعمل هذه التقنية من خلال السماح للمستخدمين بتحميل الوسائط الرقمية، و يتم تحليلها تلقائيًا بعد ذلك من أجل التحديد من خلال النظام ما إذا كانت الوسائط مزيفة

المميزات الرئيسية :Sentinel

- اكتشاف التزييف العميق المستند إلى الذكاء الاصطناعي.
- تستخدم من قبل المنظمات والحكومات الرائدة والمتقدمة في الدول المتقدمة.
- يسمح للمستخدمين بتحميل الوسائط الرقمية لتحليلها.



الشكل (2) يوضح كاشف التزييف العميق - (يحي دهشان. (2023)

3- كاشف التزييف العميق FakeCatcher (11) :

من إنتاج شركة Intel ويستخدم أجهزة وبرامج Intel يمكن لهذه التقنية اكتشاف مقاطع الفيديو المزيفة بمعدل دقة يبلغ 96٪ ، مما يؤدي إلى إرجاع النتائج في أجزاء من الثانية تم تصميم الكاشف بالتعاون مع Umur Ciftci من جامعة ولاية نيويورك في Binghamton ، ويستخدم أجهزة وبرامج Intel ، ويعمل على خادم ويتفاعل من خلال منصة على شبكة الإنترنت, يبحث FakeCatcher عن أدلة حقيقية في مقاطع فيديو حقيقية ، وتقييم ما يجعلنا بشرًا - "تدفق الدم" الدقيق في وحدات البكسل في مقطع فيديو عندما تضخ قلوبنا الدم ، يتغير لون عروقنا. يتم جمع إشارات تدفق الدم هذه من جميع أنحاء الوجه وتقوم الخوارزميات بترجمة هذه الإشارات إلى خرائط زمانية مكانية. بعد ذلك، باستخدام التعلم العميق، يمكنه اكتشاف ما إذا كان مقطع الفيديو حقيقيًا أم مزيفًا على الفور.

المميزات الرئيسية لكاشف التزييف العميق في الوقت الحقيقي:

- يمكنه اكتشاف مقاطع الفيديو المزيفة بمعدل دقة 96٪.
- إرجاع النتائج بالميلي ثانية.
- يستخدم تقنية "تدفق الدم" الدقيقة في بكسلات الفيديو لاكتشاف التزييف العميق.

4- اكتشاف التزييف العميق باستخدام عدم تطابق Phoneme-Viseme (12):

هذه التقنية المبتكرة ، تستغل حقيقة أن البصمات ، التي تشير إلى ديناميكيات شكل الفم ، تكون أحيانًا مختلفة أو غير متوافقة مع الصوت المنطوق, هذا التناقض هو عيب شائع في التزييف العميق ، حيث يكافح الذكاء الاصطناعي غالبًا لمطابقة حركة الفم مع الكلمات المنطوقة, تستخدم تقنية عدم التطابق Phoneme-Viseme خوارزميات متقدمة للذكاء الاصطناعي لتحليل الفيديو واكتشاف التناقضات، يقارن حركة الفم (البصمات) بالكلمات المنطوقة (الصوتيات) ويبحث

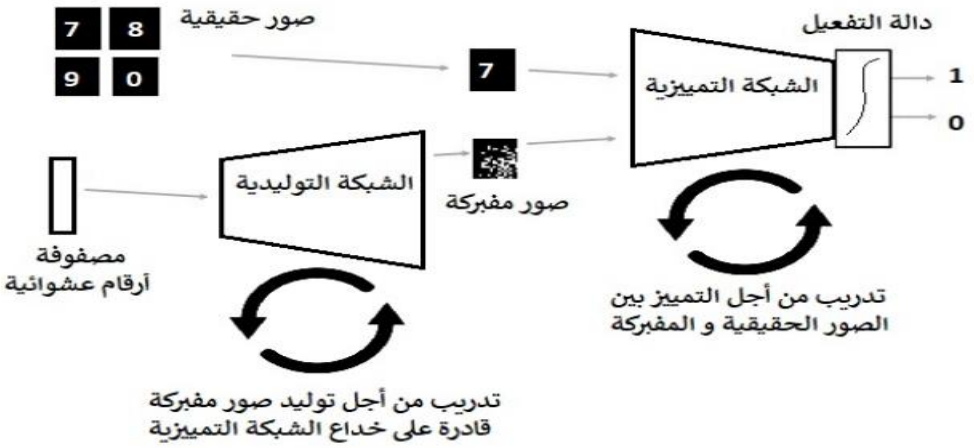
عن أي عدم تطابق, إذا تم اكتشاف عدم تطابق ، فهذا مؤشر قوي على أن الفيديو مزيف عميق.

المميزات الرئيسية لاكتشاف التزييف العميق باستخدام عدم تطابق :Phoneme-Viseme 13

1- يستغل التناقضات بين البصمات والصوتيات في التزييف العميق.

2- يستخدم خوارزميات الذكاء الاصطناعي المتقدمة لاكتشاف حالات عدم التطابق.

3- يعطي مؤشراً قوياً على التزييف العميق إذا تم الكشف عن عدم تطابق.



الشكل (3) يوضح طريقة الالية كشف التزييف العميق - (يحي دهشان. (2023)

خاتمة البحث:

تناول البحث موضوع الجرائم والانتهاكات الإلكترونية من خلال إستخدام تطبيقات وخوارزميات الذكاء الاصطناعي باعتبارها ظاهرة تفشت في المجتمعات الحديثة ونالت من المجتمعات النامية مثلما نالت من المتقدمة، نظراً إلى أن تقنيات التزييف العميق أصبحت أكثر تقدماً ويمكن الوصول إليها، فقد تصاعدت المخاطر المرتبطة بها عالمياً، مما زاد من إمكانية تعرض الأفراد والمنظمات والدول لهذه المخاطر وتسبب مجموعة من الاحتيالات وتتمثل المشكلة في كيفية تحديد التزييف والتزوير وإجراء التدابير التقنية والتعرف على الحلول والمعالجات تساعد في الحماية. ونظراً إلى التأثير المجتمعي العميق للتزييف العميق، فمن الأهمية من وجه نظر الباحثون بما كان من توجيه وتطوير تطبيقات إيجابية وبنَّاءة مع تخفيف المخاطر المرتبطة بالمشاكل.

يمكن تلخيص أهم النتائج التي توصل اليها الباحثون في مجموعة نقاط وهي:

- تمثل أدوات وتقنيات اكتشاف التزييف العميق التي تم شرحها من خلال الباحثين وما توصل له البحث في إستخدام خوارزميات الذكاء الاصطناعي المتقدمة لتحليل واكتشاف التزييف العميق بدقة, تقدم كل أداة وتقنية نهجًا فريدًا لاكتشاف التزييف العميق ، بدءًا من تحليل العناصر الرمادية الدقيقة لمقطع فيديو إلى تتبع تعابير الوجه وحركات الأشخاص و درجة ثقة في الوقت الفعلي تشير إلى ما إذا كان قد تم التلاعب بالصورة الثابتة أو الفيديو هذه الأدوات ، إلى جانب الأدوات الأخرى

التي تم الوصول لها من خلال الباحثون، تقود الي التوصل الي نتائج تساهم في التعرف علي التزييف العميق ومواكبة تقدم التكنولوجيا الكامنة وراء تقنية التزييف العميق، مما يساعد على ضمان أصالة وثقة المعلومة.

- توصل الباحثين الي أن مشكلة التزييف العميق واستخدام خوارزميات متقدمة للذكاء الاصطناعي اصبحت مهدد ومشكلة حقيقة تواجه عالمنا اليوم واصبحت الحاجة إلى أدوات وتقنيات فعالة للكشف عن التزييف العميق مع استمرار تقدم التكنولوجيا الكامنة وراء تقنية التزييف العميق، يجب أن تتقدم أيضًا أساليبنا في الكشف.

- إن التكنولوجيا فقط لا تكون حل في مشكلة التزييف العميق، ويجب التركيز على التعليم والوعي والتثقيف للمجتمعات والاطلاع بأحدث التطورات في تكنولوجيا التزييف العميق والكشف، بحيث يمكن لعب دور في مكافحة هذا التهديد.

- كما يجب التوعية بمجموعة من النقاط الهامة المتمثلة في الآتي:

- ✓ يجب على الحكومات والشركات التوعية والاستفادة من تقنيات الذكاء الاصطناعي للكشف عن البرمجيات الخبيثة وفيديوهات التزييف العميق، وتطوير أدوات متقدمة للكشف عن التلاعب في المحتوى الرقمي والتعاون الدولي.

آليات التصدي لهذه العمليات ينجم من خلال تعزيز وعي الأفراد، حيث يجب على الأفراد أن يكونوا على دراية بمخاطر الذكاء الاصطناعي في الجرائم الإلكترونية والتزييف العميق، وأن يتبعوا ممارسات أمان رقمية مثل التحقق من مصادر الأخبار، والاستثمار في التقنيات الدفاعية.

تتلخص توصيات الباحثون في مجموعة من النقاط يتم توضحيها في الاتي:

- إقامة مؤسسات بحثية داخل وحدات مكافحة جرائم الذكاء الاصطناعي تهتم بالأمن الدولي الإلكتروني، والتعامل مع التطورات التقنية التي تؤدي إلى تطور وسائل التزييف والتزوير العميق.

- بعد تحديد تقنيات التزييف العميق وتأثيرها على المجتمع يجب رفع مستوى الوعي بالتطبيقات الخبيثة وغير الخبيثة لتقنيات التزييف العميق.

- بعد تحديد إستراتيجيات تخفيف المخاطر وتمكين الجهات التنظيمية والجهات الحكومية، يجب تقديم تدابير وقائية لتحديد ومكافحة تقنيات التزييف العميق.

- تعزيز التعليم الفعَّال والقدرة على مواجهة إساءة استخدام تقنية التزييف العميق.

- المشاركة الجماعية للجهات الحكومية، والمنظمات ومراكز الأبحاث والجامعات، في رسم السياسات لمنع التزييف العميق والجرائم المستترة والظاهرة، ووضع قوانين وتدابير إجرائية.

جدول قائمة الاختصارات

قائمة الاختصاراتICD / ITKE		
الذكاء الاصطناعي	(AI)	Artificial Intelligence
أمن المعلومات	(IS)	Information security
شبكة خصوصية توليدية	(GAN)	Generative adversarial Networks
الثغرات الأمنية	(XSS)	Cross-Site Scripting

المصادر والمراجع:

1- محمد عبدالحليم حافظ، ٢٠٢٤ اتجاهات الجمهور نحو استخدام الشركات لتقنية التزييف العميق (Deep fake) في إعادة تقديم الإعلانات القديمة بصورة حديثة- جامعة الأزهر، مجلة البحوث الإعلامية.

2- محمد الصاوى، 2023 تكنولوجيا التزييف العميق دراسة بحثية حول الجوانب المظلمة للذكاء الاصطناعي المعهد العالي للفنون التطبيقية- التجمع الخامس، مجلة العمارة والفنون والعلوم الإنسانية.

3- مركز الإمارات للدراسات والبحوث الإستراتيجية ,2023, تقرير "تحديات التزييف العميق لمصداقية المعلومات وسبل معالجتها".

4-علاء الدين منصور مغايرة 2023جرائم الذكاء الاصطناعي وسبل مواجهتها:ء جرائم التزييف العميق نموذجا-المجلة الدولية للقانون جامعة قطر.

5- نحو بناء نظم لإدارة حماية المعلومات ايزو 27001 في المؤسسات الجزائرية، المؤتمر الدولي الثاني للذكاء الاقتصادي حول "اليقظة الاستراتيجية ونظم المعلومات في المؤسسة الاقتصادية"، ايام30/29افريل 2014، جامعة عنابة.

1- Qadim, J. (2024). altaathir alsalbiu litiqniat altazyif aleamiq ealaa sumeat alshakhsiaat albarizat ealaa minasaat altawasul alaijtimaeii dirasatan tahliliatan ealaa eayinat min alfidyuhat almufabraka. majalat aleulum wafaq almaearifa.

2- Hamad Allah, S. (2024). aistikhdam tiqniaat aldhaka' alaistinaeii waltazyif aleamiq lilmaelumat dirasatan mushiatan ealaa madaa mumarasat al'iielamiiyn alsuwdaniiyn liltatbiqat alraqamiat fi kashf almuhtawaa alzaayif lishabakat altawasul alaijtimaeii. majalat kuliyat aladab jamieat Om Dirman al'ahliati.

3- Galal, A. (2024). misdaqiat alsuwrat al'iielamiat fi zili tatawur tiknulujya aldhaka' aliastinaeii waltazyif aleamiqi. majalat Aleimarat walfunun waleulum al'iinsaniati.

3- مواقع الكترونية:

- microsoft.com/ar/security/business/zerotrust/maturity-model-assissment-coolly/account/
- http://portal.aridmy/ar-ly/account/ ly/account

* **المؤلف المرسل.**

* **Corresponding author**.

الهوامش:

1 _ يحي إبراهيم دهشان. (2023)، المسئولية الجنائية عن جرائم الذكاء الاصطناعي

2 _ يحي إبراهيم دهشان. (2023)، المرجع السابق.

3 - إيهاب خليفة ، التهديد المتصاعد للخداع العميق2019 .

4 _ إيهاب خليفة ، التهديد المتصاعد للخداع العميق2019

5 _ سارة عبدالعزيز. (2020)

6 - شبكة قنوات CNN

7 _ محمد الصاوى، 2023 تكنولوجيا التزييف العميق

8 _ محمد الصاوى، 2023 مرجع سابق.

9 -علاء الدين منصور مغايرة 2023

10 - علاء الدين منصور مغايرة 2023

11 _ علاء الدين منصور مغايرة 2023

12 - علاء الدين منصور مغايرة2023

13 _ يحي دهشان. (2023)