Comprehensive Journal of Science
Volume (11), Issue (42), (Sapt, 2026)
ISSN: 3014-6266

مجلة العلوم الشاملة
المجلد (11) العدد 42 سبتمبر 2026
ردمد: 3014-6266

الذكاء الاصطناعي و التزييف العميق ومخاطرهما على الأمن القومي
دراسة تحليلية في التهديدات وسبل المواجهة

مصباح بلعيد مصباح حدود[1] ، عثمان ميلاد سالم عبدالكريم [2]
[1]قسم تقنيات الحاسوب، المعهد العالي للعلوم والتقنية ، قصر خيار ، ليبيا
[2] قسم تقنيات الحاسوب، المعهد العالي للعلوم والتقنية ، تامزاوة ، الشاطي ، ليبيا
[1]musbah.blizzard@gmail.com , [2]Oth.abdulkarim@gmail.com

Artificial Intelligence, Deepfake and Their Risks to National Security: An Analytical Study of Threats and Countermeasures

Musbah Belaid Musbah Haduad[1] , Othman Melad Salim Abdulkarim[2]
[1]Higher Institute of Science and Technology , Gasr Khiar, Libya
[2]Higher Institute of Science and Technology-Tamzawa Alshati-libya

تاريخ الاستلام:2026/07/23 –تاريخ المراجعة:2026/07/25– تاريخ القبول: 2026/08/20– تاريخ للنشر : 6/9/ 2026

الملخص

أدى التطور المتسارع في تقنيات الذكاء الاصطناعي إلى ظهور محتوى رقمي شديد الواقعية يُنتج أو يُعدّل بواسطة خوارزميات التعلم العميق، ويُعرف هذا المحتوى باسم **التزييف العميق** أو **Deepfake**. ويشمل التزييف العميق الصور ومقاطع الفيديو والتسجيلات الصوتية والنصوص التي تُنسب إلى أشخاص أو مؤسسات بصورة غير حقيقية .ولم يعد التزييف العميق مشكلة تقنية أو إعلامية فحسب، بل أصبح تهديدًا متعدد الأبعاد يمس الأمن القومي والاستقرار السياسي والثقة العامة والأمن السيبراني والعمليات العسكرية.

تهدف هذه الدراسة إلى تحليل مفهوم التزييف العميق وعلاقته بالذكاء الاصطناعي، وبيان أبرز مخاطره على الأمن القومي، خاصة في مجالات التضليل السياسي، والتأثير في الانتخابات، والحرب النفسية، والحروب الهجينة، والاحتيال السيبراني، والابتزاز، وزعزعة الثقة في المؤسسات .كما تتناول الدراسة التحديات التقنية والقانونية التي تواجه اكتشاف التزييف العميق، وتقترح مجموعة من الإجراءات الوقائية والمؤسسية والتشريعية للحد من مخاطره. وتوصلت الدراسة إلى أن التزييف العميق يمثل تهديدًا استراتيجيًا لأنه لا يقتصر على إنتاج معلومات كاذبة، بل يمكن أن يؤدي إلى إضعاف قدرة المجتمع على التمييز بين الحقيقة والاختلاق. ولذلك فإن مواجهته تتطلب استراتيجية وطنية شاملة تقوم على استخدام الذكاء الاصطناعي الدفاعي، والتحقق الرقمي، والتشريعات المناسبة، والتعاون الدولي، ورفع مستوى الوعي الإعلامي والرقمي.

الكلمات المفتاحية :التزييف العميق، الذكاء الاصطناعي، الأمن القومي، التضليل الإعلامي، الحرب الهجينة، الأمن السيبراني، الذكاء الاصطناعي التوليدي.

1.المقدمة

يشهد العالم تغيرًا واسعًا في طبيعة إنتاج المعلومات وتداولها نتيجة التطورات المتسارعة في الذكاء الاصطناعي، ولا سيما تقنيات التعلم الآلي والتعلم العميق والذكاء الاصطناعي التوليدي. وقد أصبح بالإمكان إنشاء صور وأصوات ومقاطع فيديو تحاكي الأشخاص الحقيقيين بدرجة عالية من الواقعية، رغم أن هذه المواد لم تحدث في الواقع أو تعرضت لتعديلات جوهرية[1].

ويُعد التزييف العميق أحد أبرز تطبيقات الذكاء الاصطناعي ذات الاستخدام المزدوج؛ إذ يمكن استخدامه في مجالات مشروعة، مثل التعليم والسينما والمحاكاة والتدريب، كما يمكن توظيفه في الاحتيال والتشهير والتضليل السياسي والعمليات النفسية والهجمات السيبرانية [2]. وتكمن خطورته الأساسية في أن الجمهور قد يواجه صعوبة في اكتشاف المحتوى المصطنع بالاعتماد على المشاهدة أو الاستماع وحدهما.

وقد انتقل التزييف العميق من نطاق الترفيه إلى المجال السياسي والأمني والعسكري. فمن الممكن إنتاج تسجيلات مزيفة لمسؤولين أو قادة عسكريين، أو تركيب تصريحات لم تصدر عنهم، أو إنشاء مقاطع تهدف إلى إثارة الذعر أو التأثير في الرأي العام أو إرباك المؤسسات في أثناء الأزمات [3].

ومن منظور الأمن القومي، لا يقتصر الخطر على نشر خبر كاذب، بل يمتد إلى التأثير في إدراك المجتمع للواقع، وتقويض الثقة بالمؤسسات، وتعطيل عملية اتخاذ القرار، وزيادة الاستقطاب السياسي والاجتماعي. كما أن انتشار التزييف العميق قد يؤدي إلى التشكيك في التسجيلات الحقيقية، إذ يستطيع الشخص المتهم بارتكاب فعل أو الإدلاء بتصريح حقيقي أن ينكر ذلك بحجة أن التسجيل مزيف[4].

2.مشكلة الدراسة

تتمثل مشكلة الدراسة في أن القدرات التقنية الخاصة بإنتاج التزييف العميق تطورت بسرعة تفوق قدرة المؤسسات الحكومية والقانونية والإعلامية على كشفه وتنظيمه. وقد أدى ذلك إلى ظهور مجموعة من التحديات، من أهمها:

- صعوبة التمييز بين المحتوى الحقيقي والمحتوى المصطنع.
- سرعة انتشار المحتوى المزيف مقارنة بسرعة التحقق منه.
- إمكانية استخدام التزييف العميق ضد القادة والمسؤولين والمؤسسات العسكرية.
- توظيفه للتأثير في الانتخابات والرأي العام.
- استخدامه في عمليات الاحتيال والهندسة الاجتماعية.
- ضعف الأطر القانونية المتعلقة بإنتاج المحتوى المزيف ونشره.
- احتمال فقدان الجمهور الثقة حتى في الأدلة الحقيقية[2].

ومن هنا تبرز الحاجة إلى دراسة التزييف العميق باعتباره تهديدًا للأمن القومي، وليس مجرد ظاهرة إعلامية أو تقنية.

3.أسئلة الدراسة

تسعى الدراسة إلى الإجابة عن الأسئلة الآتية:

1. ما مفهوم التزييف العميق، وما علاقته بالذكاء الاصطناعي؟
2. ما أبرز المخاطر التي يفرضها التزييف العميق على الأمن القومي؟
3. كيف يمكن توظيف التزييف العميق في التضليل السياسي والحروب الهجينة؟
4. ما التحديات التقنية والقانونية التي تواجه كشف التزييف العميق؟
5. ما الإجراءات المناسبة للحد من مخاطر التزييف العميق؟

4.أهداف الدراسة

تهدف الدراسة إلى:

1. توضيح مفهوم التزييف العميق ومكوناته التقنية.
2. تحليل العلاقة بين الذكاء الاصطناعي والتزييف العميق.
3. تحديد المخاطر السياسية والعسكرية والاقتصادية والاجتماعية للتزييف العميق.

4. بيان دوره في التضليل الإعلامي والحرب النفسية والهجمات السيبرانية.
5. تحليل صعوبات الكشف والرد على المحتوى المزيف.
6. تقديم توصيات عملية لمواجهة هذه المخاطر.

5.منهجية الدراسة

تعتمد الدراسة على **المنهج الوصفي التحليلي**، وذلك من خلال وصف ظاهرة التزييف العميق وتحليل أبعادها التقنية والسياسية والأمنية. كما تستفيد من منهج تحليل المخاطر لتحديد مصادر التهديد، والجهات المحتملة لاستخدام التزييف العميق، والقطاعات المستهدفة، والنتائج المترتبة على استخدامه.

وتستند الدراسة إلى مجموعة من الكتب والأبحاث العلمية والتقارير المتخصصة الصادرة عن مراكز بحثية ومنظمات دولية، مع استخدام أسلوب الترقيم في الإشارة إلى المراجع داخل النص.

6.مفهوم الذكاء الاصطناعي والتزييف العميق

6.1. مفهوم الذكاء الاصطناعي

الذكاء الاصطناعي هو مجموعة من الأساليب والأنظمة الحاسوبية التي تمكن الآلات من تنفيذ مهام تتطلب عادةً قدرات بشرية، مثل التعلم، والتحليل، وفهم اللغة، والتعرف على الصور، والتنبؤ، واتخاذ القرار.

ويُعد التعلم الآلي أحد الفروع الأساسية للذكاء الاصطناعي، حيث تتعلم الأنظمة من البيانات بدلًا من الاعتماد الكامل على تعليمات برمجية ثابتة. أما التعلم العميق، فهو أحد أنواع التعلم الآلي ويعتمد على شبكات عصبية اصطناعية متعددة الطبقات قادرة على معالجة كميات كبيرة من البيانات واكتشاف الأنماط المعقدة[5].

6.2.مفهوم التزييف العميق

التزييف العميق هو محتوى رقمي يُنتج أو يُعدّل باستخدام تقنيات الذكاء الاصطناعي، بحيث يظهر شخص حقيقي وكأنه قال أو فعل شيئًا لم يقله أو يفعله في الواقع [1].

وقد يتخذ التزييف العميق الأشكال الآتية:

- استبدال وجه شخص بوجه شخص آخر.
- تقليد صوت مسؤول أو شخصية عامة.
- تعديل حركة الشفاه أو تعبيرات الوجه.
- إنشاء فيديو لشخصية لم تقل التصريحات المنسوبة إليها.
- تركيب صور أو مقاطع حقيقية مع عناصر مصطنعة.
- إنتاج تسجيلات صوتية تستخدم في الاحتيال أو الابتزاز.

6.3.التقنيات المستخدمة في إنتاج التزييف العميق

تعتمد صناعة التزييف العميق على عدد من تقنيات الذكاء الاصطناعي، ومن أبرزها:

أ. الشبكات التوليدية الخصمية

تعتمد الشبكات التوليدية الخصمية على نموذجين رئيسيين: نموذج مولد ينتج محتوى اصطناعيًا، ونموذج مميز يحاول التمييز بين المحتوى الحقيقي والمصطنع. ومن خلال التدريب المتكرر يصبح المحتوى الناتج أكثر واقعية[6].

ب. المشفرات التلقائية

تُستخدم المشفرات التلقائية في تحليل ملامح الوجه وإعادة إنتاجها، بما يسمح بتركيب وجه شخص على جسد شخص آخر.

ج. تقنيات استنساخ الصوت

تستطيع بعض الأنظمة تحليل عينة قصيرة من صوت الشخص ثم إنتاج جمل جديدة بصوته ونبرته، الأمر الذي يفتح المجال أمام عمليات انتحال الشخصية والهندسة الاجتماعية.

د. نماذج الذكاء الاصطناعي التوليدي

تسمح النماذج الحديثة بإنشاء محتوى نصي وصوتي ومرئي من خلال أوامر قصيرة، الأمر الذي أدى إلى انخفاض تكلفة إنتاج التزييف العميق وسهولة استخدامه [7].

7.تطور ظاهرة التزييف العميق

مرت ظاهرة التزييف العميق بعدة مراحل. ففي البداية كان تعديل الصور ومقاطع الفيديو يتطلب مهارات تقنية وبرامج متخصصة، وكانت آثار التلاعب واضحة نسبيًا. ومع ظهور التعلم العميق أصبح بالإمكان تدريب النماذج على عدد كبير من الصور والتسجيلات الخاصة بشخص معين، ثم إنتاج محتوى يحاكيه بدرجة أكبر من الواقعية [2].

أما المرحلة الأحدث فتتمثل في إتاحة أدوات الذكاء الاصطناعي التوليدي للجمهور العام، بحيث أصبح إنتاج الصور والأصوات والفيديوهات المصطنعة ممكنًا دون الحاجة إلى خبرة تقنية متقدمة. وقد أدى ذلك إلى توسيع دائرة الجهات القادرة على استخدام التزييف العميق، لتشمل الأفراد والجماعات الإجرامية والجهات السياسية والفاعلين الدوليين[8].

8.مخاطر التزييف العميق على الأمن القومي

يعتبر التزييف العميق من أهم الوسائل أو الطرق الحديثة التي تستخدم من بعض الافراد من اجل انشاء محتوي قريب للواقع بدرجة كبيرة جدا. وهدا المحتوي قد ينتج بيانات مظللة للواقع. مما يُسي للفراد والمجتمعات. ومن اهم هدة المخاطر هي :

8.1.التأثير في الاستقرار السياسي

يمكن استخدام التزييف العميق لإنتاج مقاطع منسوبة إلى مسؤولين أو قادة سياسيين، تتضمن تصريحات تحريضية أو قرارات خطيرة أو مواقف مخالفة للسياسة الرسمية. وقد يؤدي نشر مثل هذه المقاطع إلى اضطرابات سياسية أو احتجاجات أو أعمال عنف قبل تمكن الجهات المختصة من نفيها [4].

وتزداد خطورة هذا النوع من المحتوى عندما يُنشر في أوقات الانتخابات أو الأزمات أو التوترات الاجتماعية، لأن الجمهور يكون أكثر حساسية للمعلومات السياسية وأكثر استعدادًا للتفاعل معها.

8.2.التأثير في الانتخابات

يمكن استخدام التزييف العميق خلال الحملات الانتخابية من أجل:

- تشويه سمعة المرشحين.
- إظهار مرشح وهو يدلي بتصريحات لم تصدر عنه.
- نشر مواقف سياسية مزيفة.

- تقويض ثقة الناخبين في العملية الانتخابية.
- التأثير في نتائج التصويت.
- إرباك الجمهور قبيل موعد الانتخابات [9].

ولا يشترط أن يصدق الجمهور المحتوى المزيف بالكامل حتى يحقق هدفه؛ فقد يكون الهدف هو خلق حالة من الشك وعدم اليقين، بحيث لا يعود الناخب قادرًا على التمييز بين الحقيقة والكذب.

3.8.الحرب النفسية

تستهدف الحرب النفسية معنويات السكان والقوات المسلحة والقيادة السياسية. ويمكن استخدام التزييف العميق في:

- نشر إعلان استسلام عسكري مزيف.
- تقليد صوت قائد عسكري وإصدار أوامر غير حقيقية.
- نشر مقاطع عن خسائر عسكرية وهمية.
- بث رسائل تهديد أو تحريض منسوبة إلى مسؤولين.
- إثارة الخوف والهلع بين السكان.
- إضعاف الثقة بين القيادة والقوات التابعة لها[10].

وفي أوقات النزاعات المسلحة، قد يؤدي مقطع مزيف واحد إلى رد فعل عسكري أو سياسي خاطئ، خصوصًا إذا صدر في توقيت حساس.

8.4.الحروب الهجينة

تجمع الحروب الهجينة بين الأدوات العسكرية والسياسية والاقتصادية والإعلامية والسيبرانية. ويعد التزييف العميق أداة مناسبة لهذا النوع من الحروب لأنه يستهدف الإدراك والوعي والثقة، وليس الأنظمة التقنية فقط.

وقد تستخدم جهة معادية التزييف العميق بالتزامن مع:

- الهجمات السيبرانية.
- الحسابات الوهمية.
- الحملات الإعلامية الموجهة.
- تسريب وثائق حقيقية ممزوجة بوثائق مزيفة.
- إثارة الانقسامات السياسية والاجتماعية.
- الضغط الاقتصادي والدبلوماسي [10].

ومن خلال هذا الاستخدام المركب يمكن للمهاجم أن يخلق حالة من الارتباك العام ويجعل الدولة المستهدفة تنفق موارد كبيرة في الرد والتحقق والتوضيح.

8.5.الإضرار بالثقة في مؤسسات الدولة

تقوم الدولة الحديثة على الثقة في المؤسسات الرسمية، مثل الحكومة والجيش والقضاء ووسائل الإعلام والانتخابات. وإذا انتشرت مقاطع مزيفة منسوبة إلى هذه المؤسسات، فقد يؤدي ذلك إلى تراجع الثقة بها.

كما أن كثرة التزييف قد تؤدي إلى ظاهرة خطيرة تتمثل في التشكيك في المقاطع الحقيقية. فقد ينكر مسؤول تسجيلًا صحيحًا بحجة أنه تزييف عميق، وقد يقبل الجمهور هذا الإنكار بسبب معرفته بانتشار التقنية [1].

8.6.التهديدات العسكرية والأمنية

يمكن استخدام التزييف العميق ضد المؤسسات العسكرية والأمنية بطرق متعددة، منها:

- تقليد أصوات القادة.
- إصدار أوامر عسكرية مزيفة.
- تغيير تسجيلات اجتماعات أمنية.
- نشر خرائط أو صور عسكرية مفبركة.
- انتحال هوية مسؤولين في الاتصالات.
- تضليل القوات بشأن المواقع والتحركات.

وقد يمثل هذا النوع من الاستخدام تهديدًا مباشرًا لسلسلة القيادة، خصوصًا إذا لم تكن المؤسسات تمتلك إجراءات تحقق بديلة للأوامر الصوتية والمرئية.

8.7.التهديدات الاقتصادية

يمكن أن يؤثر التزييف العميق في الأسواق المالية من خلال نشر مقاطع منسوبة إلى مسؤولين اقتصاديين أو مديري شركات كبرى. وقد يؤدي ذلك إلى:

- انخفاض قيمة الأسهم.
- إثارة الذعر في الأسواق.
- التلاعب بأسعار العملات.
- التأثير في أسعار السلع والطاقة.
- تنفيذ عمليات احتيال مالي.
- إضعاف الثقة في الشركات والمؤسسات المالية [11].

8.8.الابتزاز وانتهاك الخصوصية

يُستخدم التزييف العميق أحيانًا لإنتاج صور أو مقاطع ذات طابع جنسي أو مسيء منسوبة إلى أشخاص حقيقيين دون موافقتهم. وقد يؤدي ذلك إلى الابتزاز والتشهير والإضرار بالسمعة والحياة المهنية والاجتماعية.

وتصبح المشكلة أكثر خطورة عندما يستهدف المحتوى مسؤولين أو دبلوماسيين أو عسكريين بهدف الضغط عليهم أو التأثير في قراراتهم [12].

9.التزييف العميق والهجمات السيبرانية

لا يعمل التزييف العميق بمعزل عن الأمن السيبراني، بل يمكن أن يكون جزءًا من هجوم إلكتروني متكامل. فقد تبدأ العملية بجمع صور الشخص المستهدف وتسجيلاته من وسائل التواصل الاجتماعي، ثم تدريب نموذج اصطناعي لمحاكاة صوته أو صورته، ثم استخدام ذلك في التواصل مع موظف أو مسؤول بهدف الحصول على معلومات أو أموال [13].

ويمثل هذا الأسلوب تطورًا لهجمات الهندسة الاجتماعية والتصيد الإلكتروني، لأن المهاجم لا يعتمد فقط على رسالة مكتوبة، بل يستطيع استخدام صوت أو فيديو يبدو صادرًا عن شخص موثوق.

ومن أمثلة ذلك:

1. انتحال صوت المدير المالي لشركة.
2. مطالبة الموظف بتحويل مبلغ مالي.
3. إرسال تعليمات مزيفة إلى موظف في منشأة حيوية.

4. طلب بيانات الدخول إلى نظام حساس.
5. استخدام المعلومات المسروقة لتنفيذ هجوم أكبر.

ويعني ذلك أن التزييف العميق قد يحول العنصر البشري إلى نقطة ضعف في منظومة الأمن السيبراني.

10.تأثير التزييف العميق في المجتمع

لا تقتصر مخاطر التزييف العميق على المؤسسات الحكومية والأمنية، بل تمتد إلى المجتمع بأكمله. ويمكن أن يؤدي انتشار المحتوى المزيف إلى:

- زيادة الاستقطاب السياسي.
- إثارة النزاعات الدينية أو العرقية أو القبلية.
- نشر الشائعات.
- تقويض الثقة بوسائل الإعلام.
- إضعاف التماسك الاجتماعي.
- التأثير في الصحة النفسية للأفراد.
- زيادة معدلات الابتزاز الإلكتروني.

وتزداد احتمالات انتشار المحتوى المزيف عندما يتضمن موضوعات مثيرة للخوف أو الغضب أو الصدمة، لأن المستخدمين يميلون إلى مشاركة المحتوى العاطفي بسرعة أكبر من المحتوى الهادئ والتحليلي [14].

11.التحديات التقنية في كشف التزييف العميق

11.1.التطور المستمر لأدوات التزييف

تتحسن أدوات إنتاج التزييف العميق بصورة مستمرة، وأصبحت قادرة على معالجة عيوب كانت تساعد سابقًا في اكتشاف التلاعب، مثل عدم تزامن حركة الشفاه أو اضطراب الإضاءة أو تشوه ملامح الوجه [15].

11.2.سباق التسلح التقني

يشبه الصراع بين منتجي التزييف العميق وكاشفيه سباقًا مستمرًا. فكلما طورت الجهات المختصة خوارزميات للكشف، عمل مطورو أدوات التزييف على تعديل النماذج لتجنب اكتشافها. ولذلك لا يمكن الاعتماد على أداة واحدة في جميع الحالات[15].

11.3.صعوبة التحقق في منصات التواصل

تسمح منصات التواصل الاجتماعي بانتشار المحتوى خلال دقائق، كما أن إعادة ضغط الفيديو أو تغيير حجمه قد يؤدي إلى فقدان بعض العلامات التقنية التي تعتمد عليها أنظمة الكشف. كذلك يمكن للحسابات الآلية أن تنشر المقطع نفسه آلاف المرات.

11.4.الفارق بين سرعة الانتشار وسرعة التصحيح

ينتشر المحتوى المزيف بسرعة أكبر من سرعة التحقيق الفني أو إصدار البيانات الرسمية. وحتى إذا تم إثبات زيف المحتوى، فقد تكون الرسالة الأصلية قد وصلت إلى ملايين الأشخاص.

11.5.مشكلة التزييف العكسي

قد يؤدي انتشار التزييف العميق إلى استخدامه ذريعة لإنكار محتوى حقيقي. ولذلك فإن التكنولوجيا لا تهدد فقط مصداقية المحتوى المصطنع، بل قد تهدد قيمة الأدلة الرقمية الحقيقية أيضًا [1].

12.التحديات القانونية والأخلاقية

12.1.تحديد المسؤولية القانونية

قد يشارك في إنتاج ونشر المحتوى المزيف عدد من الأطراف، مثل المبرمج والمستخدم والجهة التي تمول الحملة والمنصة التي تستضيف المحتوى. ولذلك يجب أن تحدد القوانين مسؤولية كل طرف وفقًا لدرجة علمه وقصده والضرر الناتج عن فعله.

12.2.التوازن بين الأمن وحرية التعبير

لا ينبغي أن تؤدي مكافحة التزييف العميق إلى حظر جميع المحتويات التي تستخدم الذكاء الاصطناعي، لأن بعض الاستخدامات مشروعة، مثل الفن والتعليم والمحاكاة. ويجب أن تركز القوانين على المحتوى الذي يسبب ضررًا أو يتضمن احتيالًا أو تشهيرًا أو تحريضًا أو تدخلًا غير مشروع في الانتخابات[16].

12.3.حماية البيانات الشخصية

يعتمد إنشاء التزييف العميق على جمع صور الأشخاص وأصواتهم وبياناتهم البيومترية. ولذلك تبرز الحاجة إلى حماية هذه البيانات ومنع استخدامها دون موافقة، خاصة عندما يتعلق الأمر بالقاصرين أو الشخصيات العامة أو العاملين في القطاعات الحساسة.

12.4.الاختصاص القضائي الدولي

قد يُنتج المحتوى المزيف في دولة، ويُنشر عبر منصة موجودة في دولة ثانية، ويستهدف أشخاصًا أو مؤسسات في دولة ثالثة. وهذا يجعل ملاحقة الجناة وتطبيق القانون أكثر صعوبة، ويؤكد أهمية التعاون الدولي [17].

13.وسائل مواجهة التزييف العميق

13.1.التحقق متعدد المصادر

ينبغي عدم الاعتماد على مقطع واحد عند التعامل مع الأحداث الحساسة. ويجب مقارنة المحتوى مع:

- البيانات الرسمية.
- وسائل الإعلام الموثوقة.
- التسجيل الأصلي.
- شهود العيان.
- المعلومات الجغرافية والزمنية.
- المصادر المستقلة.

وكلما اتفقت مصادر مستقلة متعددة، زادت احتمالية صحة المعلومة.

13.2.استخدام الذكاء الاصطناعي في الكشف

يمكن توظيف الذكاء الاصطناعي في تحليل:

- حركة الوجه.

- تناسق الإضاءة والظلال.
- تزامن الصوت مع حركة الشفاه.
- الخصائص الصوتية.
- بيانات الملف الرقمي.
- تاريخ نشر المحتوى.
- مصدر الفيديو وسلسلة تداوله[15].

ومع ذلك، يجب التعامل مع نتائج هذه الأدوات باعتبارها مؤشرات تحليلية، لا أحكامًا نهائية، لأن أنظمة الكشف قد تخطئ أو تتأثر بجودة الملف.

13.3.التوقيع الرقمي وإثبات مصدر المحتوى

يمكن استخدام التوقيع الرقمي وآليات إثبات المصدر لتحديد الجهة التي أنتجت المحتوى، ووقت إنتاجه، وما إذا كان قد تعرض للتعديل. وتساعد هذه التقنيات المؤسسات الحكومية والإعلامية على بناء سجل موثوق للمحتوى الأصلي[18].

13.4.إنشاء مراكز وطنية للتحقق

تحتاج الدول إلى إنشاء مراكز متخصصة في التحقق من المحتوى الرقمي، بحيث تتعاون فيها الجهات الأمنية والإعلامية والسيبرانية والانتخابية. ويمكن أن تتولى هذه المراكز :

- رصد المحتوى المشبوه.
- تحليل حملات التضليل.
- إصدار تنبيهات سريعة.
- دعم الجهات الحكومية والإعلامية.
- تطوير قواعد بيانات للتهديدات.
- تدريب الموظفين والمختصين.

13.5.حماية المؤسسات الحكومية والعسكرية

ينبغي اعتماد إجراءات تحقق متعددة للأوامر الحساسة، مثل:

- استخدام قنوات اتصال آمنة.
- اعتماد المصادقة متعددة العوامل.
- استخدام كلمات تحقق أو رموز طوارئ.
- عدم تنفيذ الأوامر المهمة من خلال تسجيل صوتي فقط.
- تأكيد التعليمات من خلال قناة اتصال ثانية.
- تدريب العاملين على انتحال الصوت والصورة.

13.6.التوعية الإعلامية والرقمية

ينبغي تدريب الجمهور على:

- عدم مشاركة المقاطع العاجلة قبل التحقق.
- فحص الحساب الذي نشر المحتوى.
- البحث عن الخبر في مصادر متعددة.
- الانتباه إلى المقاطع التي تثير الخوف أو الغضب.
- التمييز بين الحساب الرسمي والحساب المنتحل.
- استخدام أدوات الإبلاغ عن المحتوى الضار.

13.7.التشريعات المتوازنة

ينبغي أن تجرّم القوانين الاستخدامات الضارة للتزييف العميق، مثل:

- الاحتيال المالي.
- الابتزاز.
- التشهير المتعمد.
- انتحال المسؤولين.
- التأثير غير المشروع في الانتخابات.
- التحريض على العنف.
- الإضرار بالأمن القومي.

وفي المقابل، ينبغي حماية الاستخدامات المشروعة للتقنية، مع إلزام المنتج بالإفصاح عن طبيعة المحتوى عندما يكون ذلك ضروريًا.

14.إطار وطني مقترح لإدارة مخاطر التزييف العميق

يمكن بناء إطار وطني لمواجهة التزييف العميق من خلال خمس مراحل:

المرحلة الأولى: الوقاية

وتشمل حماية البيانات، وتطوير الوعي، وتحديث أنظمة الاتصال، واعتماد آليات موثوقة لتوثيق المحتوى الرسمي.

المرحلة الثانية: الرصد

وتشمل متابعة المحتوى العام، وتحليل الحسابات المنسقة، ورصد الحملات التي تستهدف مؤسسات الدولة أو الشخصيات العامة.

المرحلة الثالثة: التحقق

وتشمل الفحص التقني، والتحقق من المصدر، ومقارنة المحتوى بالأدلة المستقلة، وتحديد درجة الثقة في النتيجة.

المرحلة الرابعة: الاستجابة

وتشمل إصدار بيانات رسمية سريعة، وإبلاغ المنصات بالمحتوى الضار، وتفعيل الإجراءات القانونية، وتقديم المعلومات للجمهور بلغة واضحة.

المرحلة الخامسة: التقييم والتعلم

وتشمل تحليل الحادثة، وتحديد نقاط الضعف، وتحديث الأدوات والإجراءات، وتدريب العاملين على سيناريوهات جديدة.

15.النتائج

توصلت الدراسة إلى النتائج الآتية:

1. التزييف العميق أحد أخطر تطبيقات الذكاء الاصطناعي ذات الاستخدام المزدوج.
2. يستهدف التزييف العميق الثقة والإدراك الجمعي، وليس الأنظمة التقنية فقط.
3. يمكن استخدامه في التضليل السياسي والتدخل في الانتخابات والحرب النفسية والهجمات السيبرانية.
4. تزداد خطورته في أوقات الأزمات والنزاعات بسبب سرعة انتشار المحتوى.
5. لا توجد أداة واحدة قادرة على كشف جميع أنواع التزييف العميق بدقة مطلقة.
6. قد يؤدي انتشار التزييف العميق إلى التشكيك في الأدلة الحقيقية.
7. تتطلب المواجهة تعاونًا بين الحكومة والمؤسسات الأمنية وشركات التكنولوجيا ووسائل الإعلام.
8. لا بد من الجمع بين الحلول التقنية والتشريعات والتوعية العامة.
9. يجب تطوير قدرات وطنية مستقلة في مجال التحقق الجنائي الرقمي.
10. ينبغي أن تتضمن خطط الأمن القومي سيناريوهات خاصة بالهجمات القائمة على التزييف العميق.

16.التوصيات

توصي الدراسة بما يأتي:

1. إدراج التزييف العميق ضمن التهديدات الرسمية للأمن السيبراني والأمن القومي.
2. وضع استراتيجية وطنية لمواجهة المحتوى الاصطناعي الضار.
3. إنشاء مركز وطني لرصد التزييف العميق والتحقق منه.
4. دعم البحث العلمي العربي في مجال الذكاء الاصطناعي الجنائي.
5. تطوير أدوات عربية لكشف التزييف الصوتي والمرئي.
6. تدريب العاملين في الدفاع والأمن والإعلام والطاقة والاتصالات على مخاطر انتحال الهوية.
7. اعتماد بروتوكولات تحقق إضافية للأوامر الحكومية والعسكرية الحساسة.
8. سن قوانين تجرّم التزييف العميق المستخدم في الاحتيال والابتزاز والتشهير والتدخل في الانتخابات.
9. إلزام المنصات الرقمية بتطوير آليات للإبلاغ عن المحتوى الاصطناعي الضار.
10. تعزيز التعاون الدولي وتبادل المعلومات حول الحملات المضللة.
11. نشر برامج للتربية الإعلامية والرقمية في المدارس والجامعات.
12. عدم إعادة نشر المحتوى المشبوه عند محاولة نفيه إلا في حدود الضرورة وبعد توضيح سياقه.
13. استخدام تقنيات التوقيع الرقمي وإثبات مصدر المحتوى في المؤسسات الرسمية.
14. إنشاء خطط اتصال حكومي للأزمات تتيح الرد السريع والدقيق على المحتوى المزيف.

17.الخاتمة

أصبح التزييف العميق أحد أبرز التحديات التي فرضها الذكاء الاصطناعي على الأمن القومي. وتتبع خطورته من قدرته على محاكاة الأشخاص والأحداث بدرجة عالية من الواقعية، ومن سهولة إنتاجه وانتشاره، ومن إمكانية استخدامه في التأثير في الرأي العام، وإرباك المؤسسات، والتلاعب بالانتخابات، ودعم العمليات النفسية والسيبرانية.

ولا يتمثل الخطر في أن يصدق الجمهور مقطعًا مزيفًا فقط، بل في أن يفقد الثقة بجميع المقاطع والتسجيلات، بما فيها الأدلة الحقيقية. ولذلك قد يؤدي التزييف العميق إلى إضعاف المجال العام، وزيادة الاستقطاب، وتعطيل الاستجابة للأزمات، وتوسيع نطاق الحروب الهجينة.

وتؤكد الدراسة أن مواجهة التزييف العميق لا يمكن أن تعتمد على أدوات الكشف التقنية وحدها، بل تحتاج إلى منظومة متكاملة تشمل التشريع، والوعي الإعلامي، والتحقق الرقمي، والأمن السيبراني، والاتصال الحكومي، والتعاون الدولي. كما يمكن توظيف الذكاء الاصطناعي نفسه في مواجهة التزييف العميق من خلال تطوير أدوات دفاعية قادرة على تحليل المحتوى وتحديد مصدره ودرجة موثوقيته.

قائمة المراجع

أولًا: المراجع العربية

[1]. تشيسني، روبرت، وسيترون، دانييل.(2019).**التزييف العميق: تحدٍ وشيك للخصوصية والديمقراطية والأمن القومي** .ترجمة عنوان البحث الأصلي *Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security*. مجلةCalifornia Law Review ، المجلد 107، ص. 1753–1819.

[2].ويسترلوند، ميكائيل.(2019).**ظهور تقنية التزييف العميق: مراجعة تحليلية** .ترجمة عنوان البحث الأصلي *The Emergence of Deepfake Technology: A Review*. مجلة: Technology Innovation Management Review، المجلد 9، العدد 11، ص. 39–52.

[3].كيتزمان، يواكيم، ولي، لويس، ومكارثي، إيان، وكيتزمان، تيموثي) .2020 .(**التزييف العميق: خدعة أم تهديد؟** ترجمة عنوان البحث الأصلي *Deepfakes: Trick or Treat?*. مجلةBusiness Horizons ، المجلد 63، العدد 2، ص. 135–146.

[4].فاكاري، كريستيان، وتشادويك، أندرو.(2020).**التزييف العميق والتضليل: أثر الفيديو السياسي الاصطناعي في الخداع والثقة بالأخبار** .ترجمة عنوان البحث الأصلي *Deepfakes and Disinformation*. مجلةSocial Media + Society ، المجلد 6، العدد 1.

[5].ميرسكي، يوفال، ولي، ونغ.(2021) .**إنشاء التزييف العميق وكشفه: دراسة مسحية** .ترجمة عنوان البحث الأصلي *The Creation and Detection of Deepfakes: A Survey*. مجلة: ACM Computing Surveys، المجلد 54، العدد 1.

[6].جودفيلو، إيان، وآخرون.(2014).**الشبكات التوليدية الخصمية** .ترجمة عنوان البحث الأصلي *Generative Adversarial Nets*. مؤتمرAdvances in Neural Information Processing Systems.

[7].يوروبول.(2022).**مواجهة الواقع: إنفاذ القانون وتحدي التزييف العميق** .ترجمة عنوان التقرير الأصلي : *Facing Reality? Law Enforcement and the Challenge of Deepfakes*.لاهاي: وكالة الاتحاد الأوروبي للتعاون في مجال إنفاذ القانون.

[8].منظمة التعاون والتنمية في الميدان الاقتصادي.(2023).**الذكاء الاصطناعي التوليدي ومستقبل المعلومات الرقمية** .تقرير حول أثر النماذج التوليدية في البيئة المعلوماتية والأمن الرقمي.

ثانيًا: المراجع باللغة الإنجليزية

[9]. Chesney, R., & Citron, D. K. (2019). Deep Fakes: A Looming Challenge for Privacy, Democracy, and National Security. *California Law Review, 107*, 1753–1819.

[10]. Westerlund, M. (2019). The Emergence of Deepfake Technology: A Review. *Technology Innovation Management Review, 9*(11), 39–52.

[11]. Vaccari, C., & Chadwick, A. (2020). Deepfakes and Disinformation: Exploring the Impact of Synthetic Political Video on Deception, Uncertainty, and Trust in News. *Social Media + Society, 6*(1).

[12]. Mirsky, Y., & Lee, W. (2021). The Creation and Detection of Deepfakes: A Survey. *ACM Computing Surveys, 54*(1), Article 7.

[13]. Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative Adversarial Nets. *Advances in Neural Information Processing Systems, 27*.

[14]. Kietzmann, J., Lee, L. W., McCarthy, I. P., & Kietzmann, T. C. (2020). Deepfakes: Trick or Treat? *Business Horizons, 63*(2), 135–146.

[15]. Mirsky, Y., & Lee, W. (2021). The Creation and Detection of Deepfakes: A Survey. *ACM Computing Surveys, 54*(1).

[16]. Maras, M. H., & Alexandrou, A. (2019). Determining Authenticity of Video Evidence in the Age of Artificial Intelligence and in the Wake of Deepfake Videos. *The International Journal of Evidence & Proof, 23*(3), 255–262.

[17]. Europol. (2022). *Facing Reality? Law Enforcement and the Challenge of Deepfakes*. The Hague: European Union Agency for Law Enforcement Cooperation.