

استخدام تقنيات التزييف العميق في جريمة الاحتيال الرقمي

Using deep fake techniques in digital fraud

جمعة محمد¹¹ جامعة البويرة، mohamed.djemaa@univ-bouira.dz

تاريخ الاستلام: 2026/01/03 تاريخ القبول: 2026/09/09 تاريخ النشر: 2026/10/01

ملخص:

مع التزايد المستمر لجرائم الاحتيال عبر مختلف الوسائط خاصة الرقمية منها مثل مواقع التواصل الاجتماعي وفي ظل الانتشار الواسع لتطبيقات الذكاء الاصطناعي الذي أصبح جزء لا يتجزأ من الاستخدامات اليومية للأفراد، جاءت دراستنا هاته بهدف تسليط الضوء على تقنية تندرج ضمن تقنيات الذكاء الاصطناعي وهي تقنية التزييف العميق، هذا الأخير أصبح وسيلة جديدة للاحتيال على الأفراد بمختلف الطرق والوسائط، وعليه نهدف إلى معرفة أهم التقنيات والأدوات التي تستعمل في عملية الاحتيال، أين سنقدم نماذج للأدوات والمهام التي تقوم بها وكذا طبيعة الاحتيال والفئات المستهدفة

كلمات مفتاحية: الذكاء الاصطناعي؛ التزييف العميق؛ الاحتيال الرقمي.

Abstract:

In light of the digital transformation imposed by the technological imperative and the change in the pattern of crime from classic to digital, fraud methods have changed and taken a more modern form, especially with the widespread spread of artificial intelligence (Ai) techniques, where we see digital fraud using artificial intelligence in general and the deep fakery technique, the latter has become very widespread, especially on social media, where it relies on a set of algorithms to generate fake images and videos through which users of these social media are defrauded.

This study aims to shed light on the deep fakery technique by identifying the most important techniques and tools used in the fraud process, where we will provide examples of the tool and the tasks it performs, as well as the nature of the fraud and the target groups.

Keywords: artificial intelligence, deepfake, digital fraud

*المؤلف المرسل: محمد جمعة

1. مقدمة

في ظل التحول الرقمي الذي فرضته الحتمية التكنولوجية وتغير نمط الجريمة المتعارف عليها من الطابع الكلاسيكي إلى الطابع الرقمي تغيرت أساليب الاحتيال وأخذت شكلا أكثر عصريّة، خاصة مع الانتشار الواسع لتقنيات الذكاء الاصطناعي **Ai**، أين أصبحنا نرى احتيالا رقميا بواسطة الذكاء الاصطناعي عامة وتقنية التزييف

العميق Deep fake ، هذا الأخير أصبح منتشرًا بشدة خاصة عبر وسائل التواصل الاجتماعي، أين يعتمد على مجموعة من الخوارزميات لتوليد صور وفيديوهات مزيفة يتم من خلالها الاحتيال على مستعملي تلك الوسائط الاجتماعية، سواء من خلال تزييف صور وفيديوهات لمنتوجات أو شخصيات عامة ومعروفة بهدف تغليب الطرف الآخر والاحتيال عليه.

قد يأخذ الاحتيال عدة أشكال مثل عرض سلع ومنتجات من قبل شخص معروف تم إنشاء فيديو مزيف له وبالتالي أخذ أموال للطرف وغيرها من الأساليب الاحتيالية التي انتشرت.

2. نظرة في المفهوم وتحديد المصطلح:

1.2. مفهوم الذكاء الاصطناعي: يعتبر الذكاء الاصطناعي من التقنيات الحديثة والمتطورة وهو مرتبط بالبرمجيات والحاسب، حيث يعتبر محاكاة للتفكير البشري ومحاولة لجعل الآلة بديلة للبشر، الذكاء الاصطناعي غير مرتبط بمجال واحد، بل يشمل العديد من المجالات والاستخدامات، حيث نراه في البحث العلمي والطب والعلوم المختلفة، تعددت مفاهيمه واختلفت حسب طبيعة الاستخدام إلا أن جل المفاهيم تصب في كونه تقنية تعتمد على الأجهزة الإلكترونية وتحاول محاكاة البشر، وفيما يلي بعض المفاهيم.

هو مجال الدراسة في علم حاسب الذي يهتم بتطوير آلة تستطيع قيام بعمليات شبيهة بعمليات التفكير الإنساني كالاستنتاج والتعلم والتصحيح.

يعرف أيضا بأنه: فرع من العالم حاسب يبحث في فهم والتطبيق التكنولوجية تعتمد على محاكاة الحاسب لصفات ذكاء الإنسان. (عبد الهادي، 2020، صفحة 20)

2.2 تعريف التزييف العميق:

كثير ما نسمع مصطلح التزييف الذي في غالب مرتبط بمفهوم التزوير والتغيير، سواء ارتبط هذا التغيير بصورة أو صوت أو نص أو غيره، هذا المفهوم كغيره من المفاهيم التي تناست مع التطور العلمي والتكنولوجي ارتبط أيضا بالحاسب والآلة وأصبحنا نرى التزييف في صورة رقمية ونمط مغاير لما كان عليه سابقا، فيما يلي تعريف التزييف.

هو عملية مادية وصورة من إحدى صور الكذب يقوم بها الشخص بغرض تغيير الحقيقة التي من شأنها إلحاق الضرر بالحقوق والمراكز القانونية للأفراد. (خضور ، 2023، صفحة 5)

التقنية التي يمكن من خلالها عمل مقاطع فيديو مزيفة لأشخاص يصعب إن لم يكن من المستحيل كشفها على الأقل بالنسبة للأشخاص العاديين وأنها معالجة صور للأشخاص وتحويلها إلى مقاطع فيديو باستخدام برامج كمبيوتر معينة، لتحول هؤلاء الأفراد إلى مشاركين في أفعال لم يساهموا في ارتكابه. (محمد سلامة ، 2022، صفحة 337)

3.2. تعريف الاحتيال الرقمي: اختلف العديد من الفقهاء في تحديد مفهوم للاحتيال كونه من المفاهيم الشاسعة خاصة في المجال الإلكتروني لكن ذلك لم يمنع من بروز بعض المفاهيم التي ربطته بالاستيلاء على الغير سواء مال أو غيره، عليه فالاحتيال هو الاستيلاء على الحياة الكاملة لمال الغير بوسيلة يشوبها الخداع تسفر عن تسليم ذلك

المال، عرف أيضا على أنه استعمال وسيلة من وسائل التدليس التي نص عليها القانون على سبيل الحصر لحمل المجني عليه على تسليم الجاني مالا مملوكا لغيره نتيجة الوقوع في الغلط.

عرفه المشرع الجزائري في قانون العقوبات على أنه كل من توصل لاستلام أو تلقي أموال، أو منقولات، أو سندات، أو تصرفات، أو أوراق مالية، أو وعود وكان ذلك بالاحتيال لطلب كل ثروة الغير أو بعضها أو الشروع فيه إما باستعمال أسماء، أو صفات كاذبة، أو سلطة خيالية، أو اعتماد مالي. (شهيرة ودنيا، ب-ت) الشائع في مفهوم الاحتيال الرقمي هو أنه اعتداء على ملكية الغير والاستيلاء عليها باستخدام أساليب رقمية وأدوات ذكية وهو مغالطة المجني عليه والتحايل عليه من خلال توهيمه بفيديوهات أو صور تبدو حقيقية وهي في الأصل مزيفة يصعب التعرف عليها بسهولة.

3. كرونولوجيا تطور الذكاء الاصطناعي والتزييف العميق:

للوهلة الأولى يتبادر لذهن الكثيرين أن الذكاء الاصطناعي وليد اليوم وأنه من التقنيات التي ظهرت في الآونة الأخيرة فقط، لكن الواقع عكس ذلك فهو يعتبر من التقنيات القديمة نوعا ما والتي كانت متواجدة لسنوات مضت، وفيما يلي بعض المحطات المهمة التي تثبت فرضية قدم استخدام الذكاء الاصطناعي في شتى المجالات.

يعود مصطلح "الذكاء الاصطناعي" إلى العالم الأمريكي جون مكارثي، (McCarthy John) الذي صاغه عام 1956. ويُعرف الذكاء الاصطناعي بأنه العلم والهندسة المختصة بصناعة آلات الذكية، وخاصة برامج الحاسوب التي تحاكي الذكاء البشري. كان من أبرز إنجازاته تطوير لغة LISP، وهي أول لغة برمجة مخصصة للذكاء الاصطناعي.

1960 قام جوزيف فيزنباوم بتطوير برنامج ELIZA ، الذي يعد من أوائل البرامج القادرة على محاكاة التفاعل البشري من خلال الحوارات النصية.

- السبعينيات: شهدت هذه الفترة ظهور النظم الخبيرة، وهي برامج قادرة على تحليل البيانات واتخاذ القرارات، مثل نظام Dendron عام 1971، الذي استخدم في التحليل الكيميائي.

- أدب الذكاء الاصطناعي: توقع الكاتب إسحاق آسي موف تطور الذكاء الاصطناعي، وأطلق مصطلح الربوت، كما وضع القوانين الثلاثة للروبوتات لمنعها من التمرد على البشر، ولاحقا أضاف القانون الصفري، الذي يمنع الروبوت من إيذاء البشرية ككل.

تفوق الحاسوب ديب بلو (Blue Deep) من IBM على بطل العالم في الشطرنج غاري كاسباروف، مما أثار مخاوف بشأن قدرات الذكاء الاصطناعي.

2002: ظهر الروبوت رومبا (Rumba) ، وهو مكنسة آلية قادرة على التنقل والتنظيف ذاتيًا، مما شكل أول تطبيق عملي للذكاء الاصطناعي في المنازل.

2010: قدمت IBM الحاسوب واطسون (Watson) ، القادر على تحليل البيانات والإجابة على الأسئلة المعقدة، مما جعله أداة مفيدة في الأبحاث والعمليات التجارية.

2011: قدمت شركة أبل المساعد الذكي سيرى (Siri) ، وهو أول مساعد افتراضي يعتمد على الذكاء

الاصطناعي ليصبح متاحا للمستخدمين العاديين.

2017: بدأت شركة وايمو (Waymo) اختبار أول سيارة أجرة ذاتية القيادة، والتي أصبحت متاحة للجمهور

في 2020 في ولاية أريزونا الأمريكية.

2017: ظهرت الروبوت صوفيا، التي حصلت على الجنسية السعودية، مما جعلها أول روبوت يمنح حقوق

قانونية.

2020 وما بعده: استمرت تطورات الذكاء الاصطناعي، مثل مشروع المجادل (Debater) من IBM، وهو

حاسوب قادر على خوض مناقشات منطقية مع البشر كما بدأ الذكاء الاصطناعي في المساهمة في إنتاج الأعمال الفنية والمقالات. (عمر ، 2023، صفحة 5)

4. استخدام التزييف العميق كأداة للاحتيال وانتحال الشخصيات: ظهرت في الآونة الأخيرة العديد من الفيديوهات عبر وسائل التواصل الاجتماعي لشخصيات بارزة ومعروفة في الوسط العام، هاته الشخصيات ظهرت تروج لمنتجات معينة وماركات معروفة بغرض عرضها وبيعها وإقناع الطرف الآخر بذلك، وبحكم شهرة تلك الشخصيات فإن المستهلك يقع في المحذور ويتعرض للخداع سواء من خلال وسائل الدفع وبالتالي يتعرض لاحتيال مالي أو من خلال المنتجات المزيفة التي تم الترويج لها على أنها منتجات أصلية وذلك كله من خلال فيديوهات مفبركة ومتقنة الصنع، لا يستطيع المستهلك التفريق بينها وبين الفيديوهات الأصلية.

هناك العديد من الطرق والأساليب التي يتبعها المحتال من أجل إنشاء فيديوهات من هذا النوع وفيما يلي

سوف نتطرق لاستخدام التزييف العميق في انتحال الشخصيات وتحرير صور وفيديوهات مفبركة.

1.4. انتحال الشخصيات العامة: تُستخدم تقنية التزييف العميق لإنتاج مقاطع تُظهر شخصيات عامة – مثل الساسة أو المسؤولين أو الإعلاميين – وهم يصرون تصريحات أو يقومون بأفعال لم تحدث في الواقع. هذا الشكل من الانتحال يحمل أبعادًا خطيرة تتعلق بالتضليل الإعلامي، والتشهير، والتأثير على الرأي العام، خاصة في السياقات السياسية والاجتماعية الحساسة.

2.4. انتحال الهويات في الجرائم الإلكترونية:

أدى تطوّر هذه التقنية إلى ظهور أنماط جديدة من الجريمة السيبرانية، حيث بات بإمكان المجرمين انتحال أصوات أو وجوه أشخاص حقيقيين بغرض ارتكاب أفعال احتيالية، مثل طلب تحويلات مالية أو ابتزاز الضحايا باستخدام محتوى مزيف. ويُعد هذا الانتحال أكثر تعقيدًا من الأساليب التقليدية، لأنه يعتمد على أدوات ذكية تتعلّم من البيانات وتُحاكي السلوك البشري بدقة.

3.4. إضفاء المصداقية في عملية الانتحال:

لقد ساهم التزييف العميق في تعزيز مصداقية الانتحال الرقمي، وجعله أكثر إقناعًا وصعوبة في الاكتشاف.

فبعد أن كان من السهل تمييز المحتوى المزيف من خلال عدم تطابق الصوت أو ملامح الوجه، باتت تقنيات الذكاء

الاصطناعي قادرة على إنتاج فيديوهات ومقاطع صوتية يصعب تمييزها عن الواقع، حتى من قبل المختصين في بعض الحالات.

5. طريقة عمل التزييف العميق:

كغيره من التطبيقات أو التقنيات المتعارف عليها فإن التزييف العميق يخضع لمجموعة من العمليات المكملية لبعضها البعض من أجل توليد فيديو أو مجموعة صورة ويكون كل ذلك استنادا للذكاء الاصطناعي أو ما يسمى بتقنية التعلم، حيث يعتمد على مجموعة من الشبكات التي مهمتها توليد وصنع فيديوهات، صور، أو حركات، فيما يلي سوف نشرح آلية العمل.

1.5. مرحلة تجميع البيانات: Collection Data

في هذه المرحلة، يتم جمع بيانات ضخمة عن الشخصين المستهدفين:

- الشخص (A) الذي سيتم تبديل ملامحه.
- الشخص (B) الذي سيتم تركيب ملامحه على (A).
- هذه البيانات تشمل صورًا وفيديوهات تحتوي على زوايا متعددة وتعبير وجه مختلفة.
- جمع صور وفيديوهات للأشخاص المستهدفين من الإنترنت أو كاميرات عالية الجودة.
- تُستخدم خوارزميات التعلم العميق لفحص وتحليل هذه البيانات الحقا.

2.5. تحليل البيانات باستخدام التشفير: Process Encoding

- يتم إدخال البيانات إلى الشبكات العصبية الاصطناعية، والتي تقوم بتحليل الصور والتعرف على ملامح الوجه.
- تقوم الخوارزمية بتحديد معالم الوجه الهامة
- مثلا: شكل العينين، الأنف، الفم، خط الفك، والحواسب.... الخ
- بعد تحليل البيانات يتم تحويل هذه المعلومات إلى تمثيل رقمي مضغوط وهو بمثابة بصمة رقمية للوجه.

3.5. فك التشفير واستبدال الوجوه: Swapping Face & Decoding

- يتم استبدال ملامح وجه (A) بملامح وجه (B) باستخدام نموذجين من خوارزمية فك التشفير
- النموذج الأول يُعيد بناء الوجه الأصلي استنادا إلى البيانات المدخلة.
- النموذج الثاني يقوم بإعادة بناء الوجه بعد استبدال الملامح بالشخص الجديد (B)
- تُستخدم تقنيات مثل GANs (الشبكات العصبية التوليدية التنافسية) لضبط جودة التغيير

4.5. تحسين التفاصيل وإضافة الواقعية: (Refinement & Processing-Post)

- بعد استبدال الوجوه هناك تحسينات ضرورية لجعل الفيديو يبدو طبيعياً مثل:
- تصحيح الإضاءة لضمان أن الوجه المركب يتناسب مع بيئة الفيديو.
- تحسين الظلال لتبدو طبيعية مع حركة الرأس.
- مزامنة تعبير الوجه مع الصوت لتكون واقعية.

- تحسين جودة الصورة باستخدام تقنيات الذكاء الاصطناعي.

5.5. أدوات وتطبيقات تدعم هذه المرحلة:

Portraits Video Deep يستخدم تقنيات تحسين التعبير وتحريك الوجه بواقعية.

Face App يضيف تحسينات تلقائية لجعل الوجه أكثر طبيعية.

Resemble.ai إنشاء أصوات واقعية.

6.5. إنتاج الفيديو النهائي (Output & Rendering):

- بعد إتمام جميع التحسينات، يتم إنتاج الفيديو النهائي بجودة عالية.

- يتم تصديره بصيغ مثل MP4 أو AVI ليكون جاهزا للنشر أو المشاركة.

- يمكن إضافة مؤثرات صوتية أو مزامنة الصوت الأصلي مع الفيديو الجديد.

6. الجرائم الناتجة عن التزييف العميق:

1.6. الاحتيال الرقمي واستغلال الهوية الافتراضية:

يُستخدم التزييف العميق في انتحال هوية شخصيات معروفة أو مسؤولين حكوميين أو رجال أعمال لإقناع

الضحايا بتحويل الأموال أو تقديم بيانات حساسة. يمكن أن يظهر ذلك في شكل:

- الاحتيال عبر البريد الإلكتروني والصوت: إرسال رسائل بريدية أو تسجيلات صوتية مزيفة تبدو وكأنها صادرة

عن جهات رسمية.

- خداع موظفي البنوك: إنشاء مقاطع فيديو مزيفة لمدرء تنفيذيين تطلب منهم تنفيذ معاملات مالية طارئة.

- التلاعب بسجلات الأمن السيبراني: تزوير مقاطع فيديو تُستخدم كدليل زائف في عمليات الاختراق أو

التحقيقات الأمنية.

2.6. الجرائم الجنسية والاعتداء على الخصوصية:

- نشر مقاطع جنسية مفبركة للمشاهير: حيث يتم تركيب وجوه شخصيات معروفة على مقاطع إباحية بهدف

الإساءة أو الابتزاز.

- إجبار الضحايا على إرسال صور ومقاطع حقيقية: من خلال التهديد باستخدام فيديوهات مزيفة تُظهرهم في

مواقف غير أخلاقية.

- التلاعب في الأدلة الجنائية: يمكن استخدام فيديوهات مزيفة لتوريط أشخاص في قضايا لم يرتكبوها، مما

يعقد عمليات التحقيق.

3.6. تزييف الأدلة القضائية والإعلامي بالعدالة:

تُمكن هذه التقنية من تزوير مقاطع فيديو تُستخدم كأدلة قانونية، مما يؤدي إلى:

- إدانة أشخاص أبرياء بناء على فيديوهات مزيفة تُظهرهم في مواقع الجرائم.

- تبرئة مجرمين حقيقيين من خلال تقديم أدلة مضللة تدحض التهم ضدهم.

- التأثير على شهود العيان من خلال تقديم مقاطع فيديو مزيفة تقلب الحقائق. (الشامي ، 2024)

4.6. تزيف محتوى الوسائط العالمية والتضليل الصحفي:

- نشر تقارير إخبارية مزيفة تُظهر مذيعين معروفين وهم يروجون لأخبار كاذبة.
- فبركة تصريحات المسؤولين الحكوميين بطريقة تجعلهم يبدوون وكأنهم يدعمون قضايا غير حقيقية.
- إنتاج مشاهد مزيفة للأحداث الجارية مثل الكوارث الطبيعية أو الحروب لتضليل الرأي العام

5.6. التلاعب بالمحتوى الترفيهي والفني:

- سرقة حقوق الملكية الفكرية عبر إنشاء مقاطع أفلام مزيفة تحتوي على ممثلين دون موافقتهم.
- إنتاج محتوى موسيقي مزيف حيث يتم تقليد أصوات الفنانين لإنتاج أغاني دون إذنهم.
- إعادة إحياء شخصيات تاريخية في أعمال سينمائية بطريقة قد تحرف سيرتهم الحقيقية. (قادم و محمد،

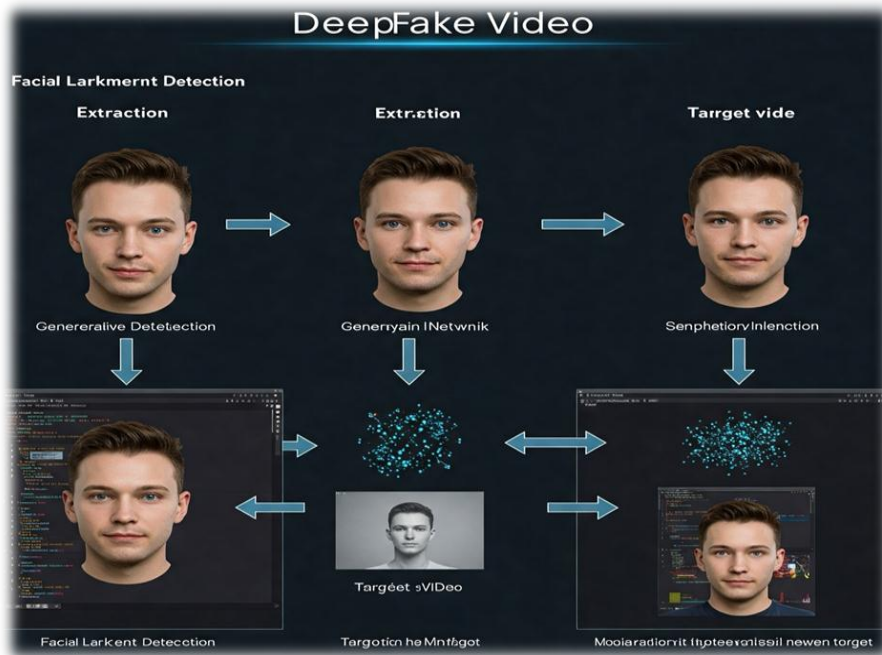
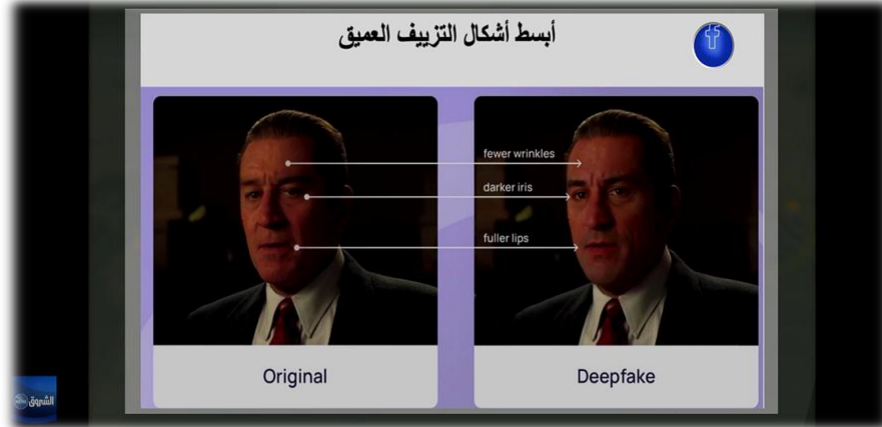
2024، صفحة 519)

7. نماذج حول التزييف العميق:

هناك العديد من الطرق والأدوات المستخدمة في عملية التزييف العميق مثلما أوضحنا فيما سبق بعض التطبيقات الأكثر استخداما وفيما يلي قمنا بجمع بعض الصور كنماذج توضيحية لعملية التزييف:



استخدام تقنيات التزييف العميق في جريمة الاحتيال الرقمي



(المصدر: جمع وإعداد الباحث)

تمثل مجموعة الصور المعروضة أعلاه نماذج لكيفية ممارسة التزييف العميق، حيث توضح الفروقات بين الصورة الحقيقية والصورة المزيفة خاصة في ملامح الوجه، والملاحظ من خلال الصور المعروضة هو صعوبة التفريق بين الصورة الأصلية والصورة المقلدة أو المزيفة إلا من خلال التركيز العالي في ملامحها وفي بعض الأحيان يستحيل التفريق بينهما إلا من خلال تقنيات خاصة بكشف الصور والفيديوهات المزيفة، نلاحظ أيضا من خلال الصور أن الجاني يحاول التركيز في تعديلاته على ملامح الوجه وحركة الشفتين وبعدها طبعا الصوت ليكون هناك تزامن مع حركة الشفاه ولا يحدث فارق زمني بين الكلام والحركة.

8. التزييف العميق بلغة الأرقام:

كما أشرنا سابقا فإن استخدامات تقنية التزييف العميق ليست وليدة اليوم بل تمتد استخداماتها لسنوات مضت، فقط يكمن الاختلاف في طبيعة العمل بها وعليها، حيث أصبحت أكثر دقة وأكثر صعوبة مما كانت سواء تعلق الأمر بالمجال العلمي والتكنولوجي أو بمجال الجريمة، حيث أصبحت هاته التقنيات مواكبة لتطور نمط الجريمة ومصاحبة لها، وعليه فيما يلي بعض الأرقام التي تثبت صحة الانتشار الواسع وحجم الاستخدامات لهاته التقنية.

ستصل قيمة السوق العالمية للتزييف العميق الناتج عن الذكاء الاصطناعي إلى 79.1 مليون دولار أمريكي بحلول نهاية عام 2024. علاوة على ذلك، وصلت إلى 1.39 مليار دولار أمريكي في عام 2023، وهو معدل نمو سنوي مركب بنسبة 37.6٪.

هناك 95,820 مقطع فيديو مزيف عميق في عام 2023 - بزيادة مذهلة بنسبة 550٪ منذ عام 2019 يتضاعف عدد مقاطع الفيديو المزيفة على الإنترنت تقريبا كل ستة أشهر؛ على سبيل المثال، كان هناك 49,081 مقطع فيديو في يونيو 2020، والتي ارتفعت إلى 85,047 فقط في ديسمبر من نفس العام هناك زيادة كبيرة بنسبة 100٪ في مقاطع الفيديو المزيفة من عام 2018 إلى عام 2019، حيث زادت إلى 14678.

بالمقارنة مع عام 2022، كان هناك ثلاثة أضعاف عدد الفيديو المزيف العميق وثمانية أضعاف عدد الفيديو القائم على الصوت

شارك مستخدمو وسائل التواصل الاجتماعي حوالي 500000 صوت وفيديو deepfakes في عام 2023، وكثير منهم سياسيون مزيّفون - مع آثار كبيرة على السياسة العالمية

ارتفع عدد المنتجات المزيفة العميقة المكتشفة في جميع أنحاء العالم عشرة أضعاف من عام 2022 إلى عام 2023: 1740٪ في أمريكا الشمالية، و1530٪ في آسيا والمحيط الهادئ، و780٪ في أوروبا، و450٪ في أفريقيا والشرق الأوسط، و410٪ في أمريكا اللاتينية.

تتمتع أجهزة الكشف البشرية بدقة 57٪ فقط في الكشف عن التزييف العميق، وهو أقل بكثير من نماذج الكشف الرائدة، والتي تبلغ دقتها 84٪.

يمكن أن تكون العملية الكاملة لإنشاء صورة أو فيديو مزيف عميق بسرعة تصل إلى 8 دقائق.

تعد "مقايضات الوجه" من بين أكثر فئات deepfake شيوعاً، مع زيادة بنسبة 704٪ من النصف الأول إلى

النصف الأخير من عام 2023 (andrada, 2024)

9. نظرة قانونية حول جرائم التزييف العميق:

في كوريا الجنوبية: تم تمرير تعديل لقانون "قضايا خاصة تتعلق بمعاقبة جرائم جنسية وحماية الضحايا

ليصبح مشاهدة أو امتلاك مواد Deepfake ذات طابع جنسي غير موافق عليه جرماً يعاقب عليه بالسجن حتى 3 سنوات أو بغرامة.

مشروع قانون تشريعات تُلزم بإيضاح أن المحتوى مولّد بالذكاء الاصطناعي (علامة مائية أو تحذير) عندما

يُستخدم لتزييف الصوت أو الصورة .

في فرنسا: تم تحديث القانون الجنائي ليشمل حظر مشاركة أي محتوى صوتي أو مرئي مولّد بالذكاء

الاصطناعي دون موافقة الشخص الظاهر فيه، مع عقوبات قد تصل إلى السجن والغرامة إذا تم النشر عبر خدمة

إلكترونية (Desmarai, June 2025).

الإمارات العربية المتحدة: قانون حماية البيانات الشخصية (PDPL) والعمليات المتعلقة بتعديل أو نشر

بيانات شخصية دون موافقة يُمكن أن تُطبّق في حالات Deepfake.

السعودية: قانون الجرائم الإلكترونية يغطي انتهاكات الخصوصية، التشهير، استخدام المعلومات الشخصية،

وقد يُستخدم لملاحقة حالات Deepfake ضمن هذه الأطر .

تونس: مرسوم رئاسي 54 Decree Law لسنة 2022 لمكافحة الأخبار الكاذبة والإشاعات، يعاقب بنشر

معلومات كاذبة جرماً عقوبة تتصل بالسجن والغرامات .

مصر دار الإفتاء المصرية أصدرت فتاوى بأن التزييف العميق الذي يُظهر أشخاصاً يفعلون أو يقولون ما لم

يفعله أو يقوله هو كذب وضلال ويُحرّم شرعاً. لكن هذا موقف ديني/أخلاقي أكثر من كونه تشريعاً مُنقّداً قضائياً .

لا يبدو حتى الآن أن يوجد قانون مصري محدد ينص صراحةً على deepfake كجريمة مستقلة، لكن هناك

قوانين حماية للسمعة والتشهير وجرائم الإلكترونية قد تُطبّق. (حكيم, 2025, pp. 2669-2742),

أما في الجزائر فهناك العديد من التشريعات التي تغطي جريمة التزييف العميق ولو أنها لم تذكره بالاسم لكنه

هناك ما يمكن تطبيقه كما يلي :

إذا كان التزييف العميق يشمل استخدام تكنولوجيا المعلومات أو الانترنت، نشر أو توزيع محتوى مزور

يُستخدم فيه اسم أو صورة شخص دون إذن، محتوى يسبب ضرراً. لكن القانون لا يذكر "deepfake" كنص

مستقل، لذا قد يكون التفسير القضائي ضرورياً لتطبيقه. الثغرة هي غياب تعريف دقيق للتزييف العميق أو

العقوبات الخاصة به، هذا القانون يختص بالجرائم المرتبطة بتكنولوجيا المعلومات والاتصال. يتضمن أحكاماً مثل

حفظ بيانات تحديد المستخدمين، إلزام مقدمي الخدمات بالتعاون مع السلطات، الاعتداءات على أنظمة معالجة

المعطيات، الجرائم الإلكترونية، قانون رقم 09 04 المؤرخ 5 أغسطس 2009 المتعلق بالقواعد الخاصة للوقاية

من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها. (القانون رقم 04-09 مؤرخ في 14 شعبان 1430 الموافق 5 أوت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها)

القانون رقم 04-09 مؤرخ في 14 شعبان 1430 الموافق 5 غشت 2009 المتضمن للقواعد الخاصة للوقاية من الجرائم المتصلة بتكنولوجيات الإعلام والاتصال ومكافحتها، مواد تحدد عقوبات للتشهير، الافتراء: مثل المادة 298 الخاصة بالتشهير ضد أفراد، وغيرها من المواد المتعلقة بالصور والإهانة .

قد يشمل بعض جوانب Deepfake إذا تم استخدام المحتوى المزيف كوثيقة أو تم الترويج له كحقيقي. إنما المشروع لا يبدو حتى الآن أنه يشير تحديدًا إلى الصور/الفيديوهات المولدة بواسطة الذكاء الاصطناعي كفتة مستقلة. لذلك هناك فجوة تشريعية إذا أراد المشرع أن يعالج "التزييف العميق" تحديدًا، هدفه يعالج حالات "الفُوق" واستعمال الوثائق المزورة، ويحاول تحديد الآليات والمعايير لتحديد من يُعتبر مسؤولًا، والتشديد على العقوبات، ومحاولات تغلب على الاحتيال باستخدام وثائق أو بيانات مزورة). المشروع المتعلق بمكافحة "الفُوق" و "استعمال المزور (Projet de loi relatif à la lutte contre le faux et usage de faux) "المعتمد من البرلمان ديسمبر 2023).

محاولة جيدة لتحديث القانون لواقع وسائل الاتصال الحديثة. لكن ما يزال لا يوجد نص يُعرّف ما هو "deepfake" أو يحدد مثلاً عقوبة خاصة لمن ينتج أو يوزع صورًا مزيفة مولدة باستخدام AI مع علمه أنها مزيفة، هذه التعديلات تضيف الوسائل التي تُستخدم - "أي وسيلة إلكترونية أو بالصورة أو الصوت" تتيح تغطية أوسع لأي محتوى مزيف يُستخدم لنشر التشهير أو الإهانة). التعديلات الحديثة على القانون الجنائي) مقالات مثل 146، 149 bis ... التي تُوسع من مفهوم الإهانة والتشهير لتشمل وسائل إلكترونية أو تصويرية ودليل الصورة والأصوات.

10. الثغرات والتحديات القانونية في الجزائر: فيما يتعلق بالتزييف العميق :

- غياب تعريف قانوني محدد لـ Deepfake لا يوجد حتى الآن في النصوص القانونية الجزائرية تعريف واضح للتزييف العميق كمفهوم مستقل، مما يترك التكييف القضائي غامضًا
-العقوبات غير مخصصة : العقوبات الموجودة للتشهير أو الاستخدام غير المشروع للبيانات الشخصية ليست مُحدّدة لعمليات التزييف العميق، فالعقوبة قد لا تكون كافية للحد من الضرر أو ردع مرتكبي مثل هذا النوع من الجريمة.

-مسألة النية والمعرفة : هل ارتكاب التزييف العميق مع وجود نية للإضرار أو مع علم بأنه مزيف؟ هذه المسائل قد تؤثر في التكييف والعقوبة، لكن القانون الحالي لا يوضحها دائمًا.

-المحتوى الجنسي أو الإباحي غير مذكور صراحةً : في حالة Deepfake ذات طابع جنسي، خصوصًا غير موافق عليه أو مع قاصر، قد يكون هناك حاجة لنصوص واضحة جداً تحظر ذلك وتحدد العقوبة.

-القوانين المتعلقة بالذكاء الاصطناعي : لا يوجد حتى الآن في الجزائر قانون شامل يُنظّم استخدام الذكاء الاصطناعي، أو خصيصًا التطبيقات التي تُولّد محتوى مزيفًا.

11. بعض التوصيات لتطوير الإطار القانوني :

- إدراج تعريف تشريعي واضح للتزييف العميق (deepfake) في القانون، يُبين ما يُقصد به من حيث الصور والفيديوهات أو الصوت المولّد بالذكاء الاصطناعي، وكيف يختلف عن التزوير "المادي" أو التقليدي.
- تحديد العقوبات الخاصة لإنشاء، نشر، أو توزيع Deepfakes ، مع درجات تشديد في حالات:
 - عندما يكون المحتوى ضارًا، تشهيريًا، يُستخدم للابتزاز، أو يخدش الكرامة.
 - عندما يتضمن قاصرين أو يكون جنسيًا.
 - عندما يُستخدم للتدخل في العملية الانتخابية أو للإضرار بالمصلحة العامة.
- إلزام المنصات الرقمية والوسائط الاجتماعية بإزالة أو تقييد المحتوى المزيف عند الإخطار، مع فرض عقوبات على الممتنعين.
- حماية الحقوق الشخصية مثل الحق في الصورة، الصوت، الكرامة، الخصوصية، السمعة، مع تمكين المتضرر من الحق في التعويض.
- موازنة ذلك، تطوير قدرات كشف التزييف العميق وتوثيق الوسائل التقنية، لتعزيز الدليل القضائي.

خاتمة:

الحديث عن تقنيات الذكاء الاصطناعي عامة والتزييف العميق خاصة يقودنا لمعرفة التغير الرهيب لأنماط الجريمة والاحتيال، فلم نعد اليوم نرى تلك الجرائم التي تعودنا على رؤيتها في طابعها التقليدي بل أصبحت تقنية بحتة خاضعة للتطور الذي فرضته العولمة والتكنولوجيا، تزايدت بفعلها مختلف أشكال الاحتيال خاصة الرقمي منه عبر وسائل التواصل الاجتماعي.

حاولنا في دراستنا هاته إبراز تقنية التزييف العميق واستخدامها في الاحتيال الرقمي وكذا تعرفنا على بعض نماذج التزييف العميق التي توضح كيفية استبدال الصوت والصورة مما يجعل التعرف على التزييف والحقيقة صعب جدا خاصة من قبل الأشخاص العاديين، للإشارة فإن الكشف عن الفيديوهات المزيفة يكون بطرق علمية وتقنيات خاصة من بينها الذكاء الاصطناعي في حد ذاته الذي يكشف الحقيقة من التزييف، لذا وجب على الجهات المخول لها مواكبة التطور العلمي والتقني خاصة في مجال الجريمة الرقمية واستعمال أحدث الوسائل لمحاربتها.

Bibliographie

الكتب:

عبد الهادي, ز. (2020). الذكاء الاصطناعي والنظم الخبيرة في علم المكتبات. القاهرة: المكتبة الأكاديمية.

محمد سلامة , ع. (2022). جريمة الانتقام الاباحي عبر تقنية التزييف العميق والمسؤولية الجنائية عنها. القاهرة، مصر.

عمر , س. (2023). الذكاء الاصطناعي. قطر: مكتبة الأكاديمية.

المجلات :

حكيم, ر. م. (2025). الجوانب القانونية للتزييف العميق. مجلة البحوث الفقهية والقانونية, المجلد 48 (العدد 48), ص ص 2669-2742.

خضور , ل. (2023). بعض تطبيقات تقنية التزييف العميق وتوظيفها التسويق والترويج المعاصر. مجلة جامعة دمشق لعلوم الهندسة, المجلد 2 (العدد 39), 5.

قادم, ج., & محمد, ا. (2024). التأثير السلبي لتقنية التزييف العميق على الشخصيات البارزة في مواقع التواصل الاجتماعي دراسة تحليلية لعينة من الفيديوهات. مجلة العلوم وافاق المعرفة, المجلد 1 (العدد 4), 519.

مراجع أجنبية:

andrada, d. r. (2024). 70 deepfake statistics your need to know.

Desmarai, A. (june2025). denmark fights back against deepfakes withcopyright protection.what other laws existe in europe.

dfgf. (fgf). gdf. fdg: dfg.

مواقع إلكترونية:

الشامي , ر. (2024). التزييف العميق يكلف شركة بريطانية عالمية 25 مليون دولار .

الاقتصادية Récupéré sur <http://cnnbusinessqrqbic.com>