سلوك حماية الخصوصية الرقمية البيومترية لدى مستخدمي تطبيقات التزييف العميق من طلبة الجامعات المصرية

د. منة الله كمال موسى دياب

مدرس بقسم الإذاعة والتلفزيون - كلية الإعلام - جامعة بني سويف

مقدمة:

شهدت الآونة الأخيرة في عصر الذَّكَاء الْاِصْطِنَاعِيّ انتشار العديد من تِقْنِيَّات التَّعَلُّم العميق، تلك التطبيقات التي تهتم بإيجاد نَظَرِيَات وخُوَارِزْمِيَّات تتيح للآلة التعلم الآلي؛ حيث تتعلم بنفسها عن طريق محاكاة الخلايا العصبية في جسم الإنسان، وهى الطريقة التي يتمكن بها الكمبيوتر من تعلم محاكاة طريقة تفكير البشر القائمة على التدريب واكتساب الخبرات، مثل فهم محتوى الصور أو الأصوات بطريقة مقاربة لطريقة فهم الدماغ البشري (Yavuzkiliç, Akhtar, Sengür & Siddique,2021)

وانتشار تكنولوجيا وتطبيقات تستوجب جمع كمٍ هائلٍ من البيانات الرَّقميَّة، وهي البيانات التي تنتج من المعاملات التي تتم عن طريق الآلة، أو أي وسيط إلكترونيّ (Dong & Zheng ,2020).

إلا أنه لم يقتصر استخدام تقنية التعلم العميق على هذا النحو؛ فقد تم –أيضًا– استخدام التطورات في مجال التعلم العميق لإنشاء برامج يمكن أن تتسبب في تهديدات للخصوصيَّة الرَّقميَّة.

واحدة من تلك التطبيقات التي ظهرت مؤخرًا معتمدة على تقنية التعلم العميق هي تقنية التَّزْييف الْعَمِيق، المعروفة باسم Deepfake هي طريقة لتعديل الفيديو اكتسبت زخمًا على مواقع التواصل الاجتماعيّ؛ حيث تسمح معالجة التَّزْييف الْعَمِيق للمستخدم باستبدال وجه الممثل على سبيل المثال في مقطع فيديو بوجه ممثل ثانٍ إذا توفرت صور كافية (مئات إلى آلاف) للممثلين، وسرعان ما حققت تقنية Deepfake شهرة في وسائل الإعلام؛ نتيجة لاستخدامها في أغراض منافية للآداب العامة حيث كانت وجوه الممثلات والسياسيين المشهورين «Deepfaked» في مقاطع الفيديو المنافية للآداب العامة الموجودة على مواقع الويب مثل,PornHub Reddit & Ahmed) .Sonuç, 2021)

كانت بداية ظهور التَّزْييف الْعَمِيق deepfake في عام 2017م عندما نشر مستخدم لموقع التواصل الاجتماعيّ Reddit مقاطع معدلة على الموقع لعدد من المشاهير، وتم الاعتماد في تلك المقاطع على خُوَارِزْمِيَّة الذَّكَاء الاصطناعي AI Algorithm لمبادلة الوجوه (Berghoff & .Twickel, 2021)

واعتمدت خُوَارِزْمِيَّة التَّزْييف الْعَمِيق على إنشاء صور ومقاطع فيديو مزيَّفة لا يستطيع البشر تمييزها عن الصور الأصلية عن طريق مجموعة من الخُوَرِزْمِيَّات يتم استخدامها على نطاق واسع في مهام التعرف على الصور وملامح الوجه وإعادة إنشاء صوت الشخص بدقة، وتصل أوجه التشابه أو التطابقات في الوجه بدقة 95.77 بالمائة (Chuang, Lei & Shiu ,2021).

ويتم مشاركة العديد من الصور ومقاطع الفيديو عبر مواقع التواصل الاجتماعيّ كل يوم، بما يهدد الخصوصيَّة الرَّقميَّة لمستخدمي هذه التطبيقات (Sedik&et.al ,2021)

ومع التزايد المتلاحق والملحوظ في إصدارات تطبيقات التَّزْييف الْعَمِيق للوجه مثل تطبيقات: Dong & Zheng ,2020) Jiggy , Reface, Face Swap Live, Zao, DeepFakeLab)، التي تعتمد على التعرف على الأشخاص عبر البيانات البيومتريَّة والتعرف الآلي على الأفراد استنادًا إلى سماتهم البيولوجيَّة والسلوكيَّة، والتي تعد بمثابة توقيعات بشرية فريدة يمكن قياسها، وقد تشمل جمع وتخزين سمات بيومتريَّة مختلفة لمستخدمي تطبيقات التَّزْييف الْعَمِيق مثل: الوجه، وقزحية العين، وبصمات الأصابع، واختراق الخصوصيَّة البيومتريَّة، والكشف عن المعلومات البيومتريَّة لمستخدمي تطبيقات التَّزْييف الْعَمِيق بما يمثل تهديدًا خطيرًا للأمن والخصوصيَّة (Wojewidka,2020).

ولعل خطورة الأمر تكمن في سياسات الخصوصيَّة وسياسة استخدام تلك التطبيقات واختراقها للعديد من المعلومات البيومتريَّة للمستخدمين، وعلى وجه التحديد تطبيقات التَّزْييف الْعَمِيق التي تقوم بإعادة تحرير الصور ومقاطع الفيديو مجانًا عن طريق تبديل وجه شخص ما بوجه شخص آخر باستخدام تِقْنِيَّات التَّعَلُّم العميق.

ويمكن وصف سلوك حماية خصوصيَّة الأفراد بأنه: إجراءات حاسوبية معينة يقوم بها الأفراد لتأمين معلوماتهم الشخصية، ويضطر الأفراد إلى الاعتماد على سلوك الحماية من أجل التأقلم وتبني السلوك للحد من المخاطر والتهديد والخطر، وفقًا لروجرز 1983(Yavuzkiliç & et al,2021).

ويتفق ذلك مع نص قانون حماية خصوصيَّة البيانات الشخصيَّة الرَّقميَّة رقم 151 لسنة 2020؛ حيث يعرف البيانات الشخصيَّة بأنها: أية بيانات متعلقة بشخص طبيعيّ محدد، أو يمكن تحديده بشكل مباشر أو غير مباشر عن طريق الربط بين هذه البيانات وأي بيانات أخرى: بالاسم، أو بالصوت، أو بالصورة، أو برقم تعريفي، أو محدد للهوية عبر الإنترنت، أو أي بيانات تحدد الهُويَّة النفسيَّة، أو الصحية، أو الاقتصاديَّة، أو الثقافيَّة، أو الاجتماعيَّة، ويعد تصميم تطبيقات بيومتريَّة أكثر تعقيدًا –تعتمد على عمليات مسح البصمات الرَّقميَّة، وفحوصات التعرف على الصور، بالإضافة إلى تحسين أداء الصور والكلام–أمر في غاية الخطورة (idsc.gov.eg.com,2021) ، وانتهاك خصوصيَّة المستخدم دون اعتبار لحقوق المستخدمين في الخصوصيَّة، والحق في حماية البيانات، والتي تعد من حقوق الإنسان الأساسية في ظل تنامي مشكلة انتشار المعلومات المضللة عبر الإنترنت (Santos& et al, 2021) .

وفي السياق ذاته تسببت تطبيقات التَّزْييف الْعَمِيق للوجه Deepfake في إثارة القلق بين الشركات التي تعتمد على أنظمة الأمان البيومتري، وذلك لأن التَّزْييف الْعَمِيق أصبح مقنعًا بشكل متزايد لخداع المستخدمين وأنظمة كشف الهُوِيَّة البيومتريَّة على حد سواء للاعتقاد بأنها أصلية (Adhikari& Panda ,2017).

ولما كانت اجراءات استخدام التطبيقات الإلكترونيَّة –عقب تحميل التطبيق عند الاستخدام– تشتمل على: سياسة الخصوصيَّة للمستخدم، وسياسة استخدام التطبيق (Newland ,2019) كما ظهرت خطورة ما تشتمل عليه تلك السياسات في العديد من المواقع والتطبيقات والشروط التي تمثل انتهاكا لخصوصيَّة المستخدم، والتي قد لا يلتفت إليها عند إنشائه لحساب على الموقع أو تحميله لتطبيقات بعض المواقع، وبموجب هاتين الاتفاقيتان تتمكن التطبيقات والمواقع من استخدام بيانات الزوار الشخصيَّة والاستفادة منها، ويحق لها استخدام البيانات الرَّقميَّة للمستخدم.

ومن هنا تتضح أهمية دافع وسلوك حماية الخصوصيَّة الرَّقميَّة لدى مستخدمي التطبيق من طلبة الجامعات المصريَّة، وتظهر المخاوف المتعلقة باختراق خصوصيَّة المعلومات والبيانات البيومتريَّة مما يدفع الطلاب –بشكل غير مباشر–إلى استخدام تدابير حماية الخصوصيَّة في خدمات الشبكات الاجتماعيَّة والتطبيقات الإلكترونيَّة للحد من المخاطر والتهديدات الإلكترونيَّة وفقا لما أظهرته الدراسات في مجال الخصوصيَّة، والتي نصت على أن المخاوف بشأن خصوصيَّة المعلومات ترتبط بإتباع تدابير حماية الخصوصية.

وهذا ما تسعى إليه الدراسة الحالية حيث تسعى إلى التعرف على طبيعة سلوك حماية الخصوصيَّة الرَّقميَّة البيومتريَّة لدى مستخدمي تطبيقات التَّزْييف الْعَمِيق من طلبة الجامعات المصرية.

مشكلة الدراسة:

باتت مقاطع الفيديو على مواقع التواصل الاجتماعيّ أداة مهمة لجذب رواد تلك المنصات، حيث تزايدت أعداد الذين يقبلون على مشاهدة تلك المقاطع ويستخدمونها ويتداولونها فيما بينهم، وتتعددت

دوافع استخدامهم لتلك التقنية ما بين: الترفيه، والسخرية، وتشويه السمعة، والاغراض المنافية للآداب العامة، وقد أدى تطور تِقْنِيَّات التَّعَلُّم العميق باستخدام الذَّكَاء الْاِصْطِنَاعِيّ إلى بزوغ ظاهرة أخرى وهي: الفيديوهات المفبركة المزيفة عبر تطبيقات التزييف العميق.

ولعل ما رصدته شركة Sensity للتكنولوجيا حول ارتفاع عدد مقاطع الفيديو المفبركة على الإنترنت –على مدى الأشهر الستة الأولى من العام الحالي 2021، حيث تضاعف عددها ليبلغ 49081 ألف مقطع فيديو (com,2020.alqarar) يبرز خطورة انتشار تقنية التَّزْيِيف الْعَمِيق من خلال مشاركات مستخدمي مواقع التواصل الاجتماعيّ لفيديوهات التَّزْيِيف الْعَمِيق وانتشارها على نطاق واسع.

ويتفق مع هذا ما أكده معهد الأمم المتحدة لبحوث نزع السلاح (UNIDIR) حول تداعيات الابتكارات التكنولوجية للذكاء الْاِصْطِنَاعِيّ على الخصوصيَّة الرَّقميَّة والأمن والثقة لعام 2021 جنيف في 25 أغسطس تحديدا بشأن ظاهرة التَّزْيِيف الْعَمِيق والثقة والأمن الدولي؛ حيث سلط الضوء على كيفية تنامي ظاهرة التَّزْيِيف الْعَمِيق وانتشار مقاطع الفيديو المزيفة، وتزايد أعداد التطبيقات، وتداعيات هذه الظاهرة على الخصوصيَّة الرَّقميَّة والأمن القومي والدولي (UNIDIR.Innovations–dialogue.com, 2021) .

وفي السياق ذاته ما أقره مجلس حقوق الإنسان 117/25، في جلسته 12 أيلول/سبتمبر 2014 بعنوان: (الحق في الخصوصيَّة في العصر الرقمي). في دورته السابعة والعشرين حول تعزيز وحماية الحق في الخصوصيَّة في العصر الرقمي، وما كشف عنه التقرير عن عدم كفاية التشريعات الوطنية حول حماية الخصوصيَّة الرَّقميَّة للأفراد، وضعف الضمانات الإجرائية، وعدم فعالية الإشراف، بما أسهم في انتشار انتهاكات في الحق في الخصوصيَّة الرَّقميَّة (Dargan& Kumar,2020)

ومع تزايد انتشار تطبيقات الذَّكَاء الْاِصْطِنَاعِيّ والتعلم العميق عبر الهواتف الذكية التي تسمح بتتبع سجل المكالمات، والملفات والبيانات البيومتريَّة على أجهزة الهاتف المحمول مثل: الصور أو مقاطع الفيديو أو الملفات الصوتية، أو وحدة التخزين الخارجية للجهاز، وإمكانية استخدام كاميرات الجهاز، والميكروفون أي وقت أثناء استخدام التطبيق، وخطورة ما يقوم به المستخدمون من تثبيت بعض التطبيقات دون قراءة شروط وأحكام الاستخدام أولاً، نتيجة لذلك أصبحت خصوصيتنا الرَّقميَّة البيومتريَّة مهددة بشكل متزايد؛ **لذا تتضح مشكلة الدراسة الحالية في التساؤل البحثي الرئيس للدراسة:** ما طبيعة سلوك حماية الخصوصيَّة الرَّقميَّة البيومتريَّة لدى مستخدمي تطبيقات التَّزْيِيف الْعَمِيق Deep Fake من طلبة الجامعات المصريَّة؟

أهمية الدراسة:

تتمحور أهمية الدراسة في عدة جوانب، أهمها:

تستمد هذه الدراسة أهميتها وفقا لعدة أوجه كما يلي:

- **الأهمية الموضوعية:** يستمد البحث أهميته الموضوعية نتيجة لحداثة الموضوع في المكتبات العربية، وتوظيف التقنيات المستحدثة في الإعلام مثل تِقْنِيَّات التَّعَلُّم العميق وتطبيقاته الحديثة،

وانتشار تطبيقات التَّزْييف الْعَمِيق؛ حيث يهتم هذا البحث بسلوك حماية الخصوصيَّة الرَّقميَّة البيومتريَّة (القياسات الحيوية) لدى مستخدمي تلك تطبيقات من طلبة الجامعات المصرية.

- **الأهمية الزمنية والمجتمعية:** يعتبر توقيت نشر هذا البحث من الأمور الحيوية في ظل انتشار مستحدثات الذَّكَاء الْإِصْطِنَاعِيّ، وتقنيات التعلم العميق، والتعلم الآلي، وجهود المجتمعات العربية والدول المتقدمة باستحداث تشريعات أمنية تُجَرّم التعدي على الخصوصيَّة الرَّقميَّة وخصوصيَّة المعلومات، بالإضافة إلى عقد المؤتمرات العلمية العالمية المتزايدة حول تطور تِقْنِيَّات التَّعَلُّم العميق ومزاياها، وكذلك آثارها السلبية وكيفية تفادي مخاطرها، وأهمية مواكبة كل ما هو جديد في دراسات الذَّكَاء الاصطناعي والخصوصيَّة الرَّقميَّة.

- **الأهمية المنهجية:** تعد هذه الدراسة من الدراسات الاستكشافية حول تقنية التعلم العميق؛ حيث تسعى الدراسة للكشف عن ظاهرة التَّزْييف الْعَمِيق في ضوء استخدام نظرية دافع الحماية PMT عبر تصميم وتطبيق مقياس دافع وسلوك الحماية البيومتريَّة لدى مستخدمي تطبيقات التَّزْييف الْعَمِيق من طلبة الجامعات المصرية.

أهداف الدراسة وتساؤلاتها:

أهداف الدراسة:

يتضح هدف الدراسة الرئيس في التعرف بسلوك حماية الخصوصيَّة الرَّقميَّة البيومتريَّة لدى مستخدمي تطبيقات التَّزْييف الْعَمِيق من طلاب وطالبات الجامعات المصريَّة، وذلك في ضوء نظرية دافع الحماية PMT وينبثق منه عدة أهداف فرعية، وهي:

- التعرف على معدلات استخدام تطبيقات التَّزْييف الْعَمِيق لدى عينة من طلبة الجامعات المصريَّة.
- التعرف على معدلات استخدام تطبيقات التَّزْييف الْعَمِيق وفقا للمتغيرات الديموغرافية لعينة الدراسة من طلبة الجامعات المصريَّة، والكشف عن الفروق بينهم في سلوك الحماية الرَّقميَّة البيومترية.
- التعرف على معدلات استخدام تطبيقات التَّزْييف الْعَمِيق وفقا لنوع الهاتف الذكي (Android، IOS) والكشف عن الفروق بينهم في سلوك الحماية الرَّقميَّة البيومترية.

تساؤلات الدراسة:

(1) هل يختلف سلوك الحماية البيومتريَّة بين الطلبة مستخدمي تطبيقات التَّزْييف الْعَمِيق، والطلبة غير مستخدمي تطبيقات التَّزْييف الْعَمِيق؟

(2) هل يختلف سلوك الحماية البيومتريَّة باختلاف جنس الفرد (ذكور، إناث) لدى مستخدمي تطبيقات التَّزْييف الْعَمِيق؟

(3) هل يختلف سلوك الحماية البيومتريَّة باختلاف موطن الإقامة (ريف، حضر) لدى مستخدمي تطبيقات التَّزْييف الْعَمِيق؟

(4) هل يختلف سلوك الحماية البيومتريَّة باختلاف نوع الجامعة (حكومية، خاصة) لدى مستخدمي

تطبيقات التَّزْييف الْعَمِيق؟
(5) هل يختلف سلوك الحماية البيومتريَّة باختلاف نظام الموبيل المستخدم (Android، IOS) لدى مستخدمي تطبيقات التَّزْييف الْعَمِيق؟
(6) هل تختلف درجة سلوك الحماية البيومتريَّة لدى مستخدمي تطبيقات التَّزْييف الْعَمِيق باختلاف الجنس (ذكور، إناث)، وطبيعة الإقامة (حضر، ريف)، ونوع الجامعة (حكومية، خاصة)، والتفاعل بينهم؟
(7) هل يختلف سلوك الحماية البيومتريَّة لدى طلبة الجامعة مستخدمي تطبيقات التَّزْييف الْعَمِيق باختلاف إجادتهم اللغة الانجليزية؟

الدِّراسات السابقة:

من خلال مسح التراث العلمي، ونظرا لحداثة ظاهرة انتشار تطبيقات التَّزْييف الْعَمِيق تبين وجود بعض الدراسات الأجنبية والعربية يمكن تصنيفها وفقا لعدة محاور متوافقة مع هدف الدراسة وتساؤلاتها:

المحور الاول: إستراتيجيات دافع سلوك حماية الخصوصيَّة الرَّقميَّة البيومترية.

المحور الثاني: دراسات تتعلق بتقنية التعرف على الوجه وتطبيقات التزييف العميق.

وفيما يلي نستعرض دراسات كل محور، ونختتم العرض بالتعقيب على الدراسات من الناحية المعرفيّة والمنهجيّة والنظريّة:

المحور الاول: إستراتيجيات دافع وسلوك حماية الخصوصيَّة الرَّقميَّة البيومتريّة

هدفت دراسة **سعد القرني (2021)** إلى قياس حجم ظاهرة اختراق الخصوصيَّة الرَّقميَّة عبر وسائل الإعلام الاجتماعيّ الجديد، وتطبيقات التواصل الاجتماعيّ وعلاقتها بالمتغيرات الديموغرافية، ومتغير أنماط التفكير، وأظهرت نتائج الدراسة وجود فروق ذات دلالة إحصائية في دوافع مشاركة المبحوثين اتجاهاتهم ومعتقداتهم مع الآخرين وفقا لمتغير نمط التفكير لديهم، ووفقا لنوع التطبيق الإلكتروني الذي يفضله المبحوثون في الإفصاح عن خصوصيَّة معلوماتهم، واهتماماتهم، وعلاقاتهم بالآخرين، وأوضحت نتائج الدراسة وجود علاقة ذات دلالة إحصائية بين نمط التفكير ونشر الخصوصيَّة عبر الإعلام الاجتماعيّ الجديد، وكذلك في ضوء أهمية سلوك حماية الخصوصيَّة الرَّقميَّة أوضحت دراسة: **حورية قاسي (2021)** حول: مخاطر انتهاك خصوصيَّة مستخدمي بعض التطبيقات الحديثة عبر الهواتف الذكية بالتطبيق على التطبيقات الصحية التي تم استخدامها في مواجهة جائحة كورونا في كل من كوريا الجنوبية وكذلك تايوان، وتُدعى: تطبيقات الإنذار لكَبْحِ انتشار عدوى فيروس كوفيد 19؛ وهدفت الدراسة إلى إيجاد نظام يحترم قوانين الخصوصيَّة الفردية، ويحمي المعطيات ذات الطابع الشخصي وفقا لقوانين الاتحاد الأوروبي؛ حيث اكتشفت مؤسسات الأمن الدولي بهذه الدول ما تضمنته تلك التطبيقات –على وجه الخصوص– من اختراق للخصوصيَّة البيومتريَّة الرَّقميَّة من خلال بيانات المرضى ومستخدمي التطبيقات، وأشارت نتائج

الدراسة إلى أهمية تواجد تدابير أمنية رقميَّة تضمن أمن المستخدم الإلكتروني لمنع تسريب البيانات أو حصول طرف ثالث عليها. وضرورة إفصاح التطبيقات منذ البداية عن كيفية استعمال بيانات المستخدم، وكيفية تخزينها أو تقاسمها مع القطاعات الصحية أو المستخدمين الآخرين، وذلك من خلال تعليمات استخدام واضحة ومختصرة، بالإضافة لإلزامية موافقة المستخدم بشكل صريح قبل جمع أي بيانات منه، واتفقت هذه النتيجة مع دراسة**Santos (2021)** حول اختراق تطبيقات الهواتف الذكية لخصوصيَّة المستخدمين، واتضحت معالم الاختراق الرقمي في نتائج هذه الدراسة في استخراج البيانات الشخصيَّة والتجسس على سمات المستخدم الحساسة من مستشعرات أجهزته المحمولة، وكذلك في الخصائص الديموغرافية، والمواصفات الجسدية وطبيعة النشاط الحركي والسلوكي للمستخدمين، وكذلك هدفت دراسة **سعد ابراهيم (2021)** إلى التعرف على بنود الحق في الخصوصيَّة الرَّقميَّة وما يتعرض له مستخدمو تطبيقات الذَّكَاء الْاِصْطِنَاعِيّ وتقنيات التعلم العميق من اختراقات أمنية دون أن يشعر المستخدم، وتوصلت نتائج الدراسة إلى العلاقة بين استخدام التطبيقات التي تعتمد على تقنيات التعرف على الوجه والانتهاكات الشخصيَّة والاجتماعية والمهنيَّة والسياسيَّة والتجارية للخصوصيَّة الرَّقميَّة لمستخدميها، وأشارت الدراسة إلى ضرورة التدخل التشريعي والقانوني لتعزيز وحماية حق المستخدم في الأمان الرقمي، وتضمنت نتائج الدراسة المعايير المهمة لضمان المعلومات الرَّقميَّة في إطار الحفاظ على الخصوصيَّة الرَّقميَّة من خلال ثلاثة معايير لضمان المعلومات، وأشارت إليها بمثلث أو ثلاثيCIA ، وهي اختصار لكل من: السرية والأمان والتوفر، وكذلك أشارت نتائج الدراسة إلى أشكال انتهاكات الخصوصيَّة الرَّقميَّة، واتضحت في: المراقبة، والاستجواب، والتجميع، وعدم الأمان، وانتهاك السرية، والإفصاح، والكشف عن البيانات البيومتريَّة الحيوية، والابتزاز، والاستيلاء، والتشويه، والتطفل. أما عن الحق في الخصوصيَّة في العصر الرقمي وتحديات الحصول عليها نجد أن دراسة **Acquisti & Loewenstein(2020)** أشارت إلى أن الأشخاص الذين يهتمون بخصوصياتهم ويتخذون خطوات لحمايتها، يستطيعون إدارة الخصوصيَّة بفعالية عبر الإنترنت، وأرجعت السبب الرئيس لعدم تمكن المستهلكين من الحصول على المستويات المرغوبة من الخصوصيَّة هو عدم فهمهم لكيفية جمع بياناتهم ونشرها واستخدامها، **ويتفق مع هذا الاتجاه** ما أشارت إليه دراسة**Furini & Prandi (2020)** حول سلوكيات المستخدمين الرَّقميَّة للتطبيقات دون دراية بمعايير الحماية الرَّقميَّة لبياناتهم البيومتريَّة؛ حيث يقوم المستخدمون بتثبيت التطبيقات الترفيهية في أغلب الأوقات دون قراءة شروط وأحكام الاستخدام؛ والنتيجة هي أن خصوصياتهم في خطر متزايد، وكذلك أشارت نتائج الدراسة أن تصور المستخدمين تجاه الخصوصيَّة البيومتريَّة أثناء استخدام تطبيقات الهواتف الذكية يتأثر بإدراك ومعرفة البيانات التي تستخدمها التطبيقات المثبتة، واشتملت إجراءات الدراسة المنهجية على مجموعة من الاستبانات حول التطبيقات المثبتة داخل هواتف 200 متطوع، وأظهرت النتائج إساءة استخدام البيانات المتعلقة بموقع المستخدم وجهات الاتصال الشخصيَّة والكاميرا وقائمة شبكة Wi–Fi وقائمة التطبيقات قيد التشغيل، وكذلك أشارت النتائج إلى أن المشاركات الإناث هن أكثر قلقًا بشأن احتمال إساءة استخدام كاميرا الهاتف الذكي، وكذلك كشفت نتائج الدراسة التحليلية بالتطبيق على 843 تطبيقًا

–مثبتا على هواتف عينة الدراسة –عن سيناريو ينذر بالخطر الذي يواجه مستخدمي التطبيقات الإلكترونيَّة دون دراية، على سبيل المثال أشارت نتائج الدراسة إلى أن 24٪ من التطبيقات المثبتة تصل إلى جهات الاتصال، و39٪ منهم ينتهك خصوصيَّة الموقع ومكان المستخدم وأن7٪ من التطبيقات المثبتة لديها حق الوصول إلى الرسائل القصيرة، وأن 56٪ من التطبيقات المثبتة لديها حق الوصول إلى الوسائط المتعددة وملفات الصور والفيديو، وكذلك الميكروفون، **بينما اختلفت مع هذه النتائج** ما أشارت اليه نتائج دراسة **صالح بن الناصري (2019)** التي تم تطبيقها على عينة من طلبة التعليم ما بعد الأساسي؛ فكان الذكور من فئة الشباب هم الأكثر عرضة لانتهاك حقوقهم الرَّقميَّة بالمقارنة بفئة الإناث؛ ويفسر تلك النتيجة بأن الأسر العمانية تعطي الثقة الكاملة للذكور أثناء استخدام وسائل التواصل الاجتماعيّ علي عكس الإناث، بالإضافة لتطرق الذكور عينة الدراسة لبعض المواقع المجانية –بطرق غير مشروعه والمخالفة للآداب العامة– على خلاف عينة الإناث التي اتسمت بالحياء في استخدام وسائل التواصل الاجتماعي، بالإضافة لغياب نشر ثقافة الحقوق الرَّقميَّة في الدول العربية مما يؤثر إيجابا على زيادة الانتهاكات الرَّقميَّة لمستخدمي وسائل التواصل الاجتماعي، وفيما يتعلق ببنود الحق في الخصوصية للمستهلك الإلكتروني وصور الاعتداء عليها فقد توصلت **دليلة ليطوش (2019)** في دراستها بشأن الحق في الخصوصيَّة الرَّقميَّة للمستهلك الإلكتروني؛ وهدفت الدراسة التعرف على مخاطر الاعتداءات على الخصوصيَّة الرَّقميَّة التي تتم عن طريق المعاملات التي يقوم بها المستهلك عبر شبكة الإنترنت كالتي تحمل معلومات تتعلق بحياته الخاصة كالاسم، وجنسيته، ومقر إقامة وطبيعة عمله، وأرقام حساباته البنكية في بعض الأحيان، وما قد ينتج عن تداول تلك المعلومات وتوظيفها واستغلالها بطرق غير مشروعه، وكذلك قد تشمل الاعتداءات الاعتداء على توقيعه الإلكتروني الذي يعتبر وسيلة يعبِّر بها المستهلك الإلكتروني عن إرادته في الالتزام بتصرف قانوني معين، وأكدت نتائج الدراسة أن الخطورة تكمن في أن بعض الاعتداءات على خصوصية المستهلك قد تحدث من خلال أشخاص خارج الحدود الوطنية وتصعب محاكمتهم، وهو ما تتسم به الجريمة الإلكترونية، وقد انتهت دراسة **محمدالمعداوي (2018)** بشأن حماية الخصوصيَّة المعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي إلى أن خطر تداول البيانات الشخصيَّة وجميع البيانات الرَّقميَّة المتعلقة بالمستخدم والتي تتضمن: اسمه الأول، واسم العائلة، وعنوان البريد الإلكتروني، وكلمة المرور، والجنس، وتاريخ الميلاد؛ وكذلك كافة المعلومات أو البيانات التي يطلبها الموقع من المستخدم الذى يرغب في التسجيل على موقع معين على شبكة الإنترنت، وكذلك ما تتضمنه من بيانات بيومتريَّة مثل بصمة الأصابع، أو الحمض النووي، وأيضا جميع المعلومات التي يكون من شأنها تمييز الأشخاص عن غيرهم مثل مكان الإقامة، والمهنة، والنوع، والسن.

المحور الثاني: دراسات تتعلق بتقنية التعرف على الوجه وتطبيقات التزييف العميق

يتم تبادل ملايين الصور ومقاطع الفيديو على الإنترنت يوميًا، وتنتشر سبل الخداع بمقاطع فيديو مزيَّفة تستخدم تطبيقات التَّزْييف الْعَمِيق، وقد هدفت دراسة **Jarvis (2021)** إلى إلقاء الضوء على

مخاطر تطبيقات التَّزْييف الْعَمِيق على الخصوصيَّة الرَّقميَّة للمستخدمين وضرورة قراءة سياسات الاستخدام وسياسات الخصوصيَّة بهدوء، وعدم الموافقة ضمنيا على كل الشروط رغبة في استخدام التطبيق لبعض الأغراض الترفيهية أو التجميلية بساطة بالإضافة لما أشارت له الدراسة عن سبب انتشار تلك التطبيقات وسلاسة إستخدامها من قبل مختلف الفئات العمرية فالأمر لا يتطلب سوى التقاط صورة «سيلفي» ذاتية بسيطة للشخص، ومن ثم يستطيع أن يجسد الشخصية الشهيرة التي يحلم بأن يتقمصها، وفي السياق ذاته كشفت دراسة **Bode (2021)** التي اعتمدت على دراسة حالة لاستكشاف عنصر التَّزْييف الْعَمِيق على فيلم مدته 3 دقائق و36 ثانية بعنوان:"Keanu Reeves Stops A ROBBERY!" تم نشره بسرعة على مواقع التواصل الاجتماعيّ مثل فيسبوك وتويتر، ولم يستطع المشاهدون تصنيف الفيديو على أنه مفبرك باستخدام تطبيق Faceswap للتزييف العميق الذي اعتمد على إعادة صياغة سياق المحتوى وتأخير وتسريع اللقطات، واستخدام المشابهين، واتفقت معها دراسة **Agarwal& Lim (2020)** حول خطورة المحتوى المفبرك لمثل هذه الصور ومقاطع الفيديو المضللة، ومع الاستخدام الواسع النطاق للهواتف المحمولة أصبحت تقنيات التحقق البيومتري شائعة في العالم، وتكمن خطورتها بشكل أساس في تخزين البيانات الحيوية الحساسة مثل: بصمات الأصابع، وقزحية العين، وقد قدمت دراسة **Chen (2021)** خُوَارِزْمِيَّة مبتكرة وفعالة في مقاطع فيديو الوجه لحماية الخصوصيَّة باستخدام PulseEdit يمكن من خلالها تجنب إساءة استخدام الخصوصية، هدفت دراسة **محمدالعثمني (2021)** التعرف على التداعيات السلبية لتقنية التعرف على الوجه على الخصوصيَّة الرَّقميَّة والحريات الفردية، وربط الأنظمة البيومتريَّة باستخدام الخصائص الفسيولوجية الفريدة، مثل: بصمات الأصابع، وهندسة اليد، وشبكية العين، والقزحية، والتوقيعات اليدوية لتحديد هوية الفرد، وتكمن مخاطر تقنيات التَّزْييف الْعَمِيق وتطبيقات التعرف على الوجه كما أوضحتها نتائج الدراسة في إمكانية سرقة البيانات الحيوية، وغياب الأطر التشريعية، والتحيُّز العرقي، وغياب الضوابط الأخلاقية، وانتهاك الخصوصية، كما أوصت الدراسة بأهمية تطوير الضوابط الأخلاقية والقانونية لتأطير تقنيات التعرُّف إلى الوجه بسبب تداعياتها السلبية على الخصوصيَّة والحريات الفردية للمستخدمين، مما يعني تزايُد الحاجة إلى تشريعات حكومية ودولية لإرساء أنظمة مُحكمة تُحدد استخداماتها المقبولة وغير المقبولة؛ لتعظيم فوائدها والحد من أخطارها، بينما هدفت دراسة **Kwok (2021)** إلى الإشارة لمخاطر الاستخدام الضار لمقاطع الفيديو المزيفة العميقة في عمليات الاحتيال والخداع وإساءة استخدام البيانات البيومتريَّة والتطورات السريعة في تقنية deepfake وتأثيرها المحتمل على انتحال الشخصيات الحقيقية ، كما كشفت دراسة **Wojewidka (2020)** عن خطر التَّزْييف الْعَمِيق على القياسات الحيوية، –وخاصة– أثناء استخدام التطبيقات بغرض الترفيه، والمحاكاة الساخرة، والأغراض الإجرامية، وفي الأمر ذاته اهتمت بعض الدراسات مثل دراسة **Mahdavifar& Ghorbani (2019)** بالتعرف على خُوَارِزْمِيَّات التعلم العميق للكشف عن البرامج الضارة وتصنيفها، واكتشاف عمليات الاختراق الرقمي للخصوصية، واشتملت هذه الطرق على عدة تطبيقات مثل تطبيقات اكتشاف البرامج الضارة، واكتشاف الرسائل غير المرغوب فيها، واكتشاف اختراقات الهواتف الذكية من خلال الكاميرا والميكروفون.

التعقيب على الدراسات السابقة:

- اعتمدت غالبية الدراسات الأجنبية على استخدام أداتي تحليل المضمون لتطبيقات التَّزْييف الْعَمِيق والاستبانة الإلكترونية، واتضح من خلال الدراسات أنها الأدوات الأكثر توظيفًا في الدراسات السابقة؛ وقد يفسر ذلك انتشار تطبيقات التَّزْييف الْعَمِيق في الآونة الأخيرة عقب انتشار جائحة كرونا، واعتماد الباحثين على الاستبانات الإلكترونيَّة بشكل مكثف.
- توصلت غالبية نتائج الدراسات الأجنبية التي اهتمت باستراتيجيات سلوك حماية الخصوصيَّة لدى مستخدمي تطبيقات التَّزْييف الْعَمِيق إلى وجود علاقة ذات دلالة إحصائية بين نمط التفكير عند مستخدمي تلك التطبيقات، وسلوك حماية الخصوصيَّة لديهم عبر وسائل الإعلام الرقمي.
- أشارت نتائج الدراسات إلى أشكال انتهاكات الخصوصيَّة الرَّقميَّة، وتمثلت في: (المراقبة، والاستجواب،التجميع، وعدم الأمان، وانتهاك السرية، والإفصاح) وكذلك شملت نتائج بعض الدراسات على أشكال انتهاك الخصوصيَّة الرَّقميَّة البيومتريَّة، تمثلت في (إساءة استخدام البيانات المتعلقة بموقع المستخدم، وجهات الاتصال الشخصيَّة، والكاميرا، والميكرفون، وقائمة شبكةWi–Fi ، وقائمة التطبيقات قيد التشغيل، وكذلك التجسس على كافة القياسات والبيانات الحيوية لدى مستخدمي التطبيقات مثل: بصمة الصوت: وبصمة العين: وبصمة الإصبع).
- ركزت بعض الدراسات على خطورة تداول البيانات الرَّقميَّة المتعلقة بالمستخدم من خلال تثبيت التطبيقات الإلكترونيَّة دون الاهتمام بقراءة إعدادات استخدام التطبيق أو إعدادات الخصوصية.
- أوضحت غالبية نتائج الدراسات دوافع استخدام الشباب لتطبيقات التَّزْييف الْعَمِيق وتمثلت في: استخدام التطبيقات بغرض الترفيه والمحاكاة الساخرة، والأغراض الإجرامية، والابتزاز.
- نظرا لحداثة ظاهرة التزييف وحداثة مفهوم الخصوصيَّة الرَّقميَّة البيومتريَّة فهناك ندرة في الدراسات العربية التي أشارت إلى هذه المفاهيم حيث؛ لم تلق اهتماما كبيرا في الدراسات العربية.
- تباينت نتائج الدراسات في تحديد العينة الأكثر انتهاكا في الخصوصيَّة البيومتريَّة الرَّقميَّة أثناء استخدام التطبيقات من حيث الجنس؛ فالبعض أشار إلى أن الذكور من فئة الشباب هم الأكثر عرضة لانتهاك حقوقهم الرَّقميَّة بالمقارنة بفئة الإناث، وتفسر الدراسات تلك النتيجة بأن الذكور عينة الدراسة يتطرقون لبعض المواقع المجانية المخالفة للآداب العامة بطرق غير مشروعه أثناء استخدام وسائل التواصل الاجتماعيّ على خلاف عينة الإناث التي اتسمت بالحياء في استخدام تطبيقات وسائل التواصل الاجتماعي، بينما أشارت نتائج بعض الدراسات أن الإناث هم الفئة الأكثر ابتزازا من قبل تلك التطبيقات –وخاصة– فيما يخص الاختراقات الحيوية البيومتريَّة وسعيهم وراء تطبيقات التزييف لأغراض تجميلية مثل الفلاتر ومحسنات الصورة.
- ارتكزت أهداف العديد من الدراسات على إيجاد وتصميم وابتكار خُوَارِزْمِيَّات مبتكرة وفعالة للتحقق من التَّزْييف الْعَمِيق في مقاطع الفيديو المزيفة وسبل الحد من الظاهرة، ومحاولة توظيف تِقْنِيَّات التَّعَلُّم العميق وتطبيقات التَّزْييف الْعَمِيق في أغراض إيجابية كإحياء الشخصيات التاريخية، أو لصناعة السينما.
- أشارت بعض الدراسات إلى مخاطر الاستخدام الضار لمقاطع الفيديو المزيفة العميقة في

عمليات الاحتيال والخداع، وإساءة استخدام البيانات البيومتريَّة والتطورات السريعة في هذه التقنية وتأثيرها المحتمل على السياحة، والشئون السياسية، والانتهاكات الأخلاقية، والاختراقات الأمنية.

فروض الدراسة:

(1) توجد فروق دالة إحصائياً في سلوك الحماية البيومتريَّة بين الطلبة مستخدمي تطبيقات التَّزْييف الْعَمِيق والطلبة غير مستخدمي تطبيقات التزييف العميق.

(2) توجد فروق دالة إحصائياً بين الذكور والإناث من مستخدمي تطبيقات التَّزْييف الْعَمِيق في سلوك الحماية البيومترية.

(3) توجد فروق دالة إحصائياً بين المقيمين في الريف، والمقيمين في الحضر من مستخدمي تطبيقات التَّزْييف الْعَمِيق في سلوك الحماية البيومترية.

(4) توجد فروق دالة إحصائياً بين طلبة الجامعات الحكومية وطلبة الجامعة الخاصة من مستخدمي تطبيقات التَّزْييف الْعَمِيق في سلوك الحماية البيومترية.

(5) توجد فروق دالة إحصائياً بين الطلبة مستخدمي هاتف من بنظام Android، والطلبة مستخدمي هاتف بنظام IOS من مستخدمي تطبيقات التَّزْييف الْعَمِيق في سلوك الحماية البيومترية.

(6) تختلف درجة سلوك الحماية البيومتريَّة لدى مستخدمي تطبيقات التَّزْييف الْعَمِيق باختلاف الجنس (ذكور، إناث)، طبيعة الإقامة (حضر، ريف)، نوع الجامعة (حكومية، خاصة)، والتفاعل بينهم.

(7) لا توجد فروق دالة إحصائياً بين الطلبة متقني اللغة الانجليزية وغير متقنيها من مستخدمي تطبيقات التَّزْييف الْعَمِيق في سلوك الحماية البيومترية.

الإطار النظري:

نظرية دافع الحماية (Protection Motivation Theory):

طور روجرز (1975) نظرية دافع الحماية PMT، التي تنص على أن دافع الفرد في الحماية من المخاطر والخطر ينبع من (الشدة المتصورة، الضعف الملحوظ، فعالية الاستجابة) وتم توسيع نموذج PMT ليشمل (الكفاءة الذاتية، تكلفة الاستجابة)، والحوافز المرتبطة بالسلوك المحفوف بالمخاطر لشرح الفشل في السلوك الوقائي (Cozma& Muturi,2021) استُخدمت النظرية فيما بعد في أكثر من (20) مجالا مختلفا متعلقا بالصحة من أجل دراسة نوايا وسلوكيات intentions and behaviours الأفراد. كما استخدمت بشكل موسع في مجال نظم المعلومات من أجل فحص كل من: سلوك الحماية في المعاملات عبر الإنترنت، ومدى وعي الموظفين في سياسات أمن المعلومات التنظيمية، والاستخدام الشخصي «الفردي» لبرامج الأمان (Haag ,Siponen & Liu, 2021) ، نظرية دافع الحماية Protection motivation theory (PMT) يتم تطبيقها عند فحص السلوك البشري «الإنساني» واستجابة الفرد لتهديد معين في أي موقف، واللبنات الأساسية لهذه النظرية تتمثل في تقييم العمليتين المعرفيتين: التهديد threat، وأساليب المواجهة coping.

فعندما يواجه الأفراد تهديداً معينا؛ فإن هناك ستة شروط conditions ستقودهم إما إلى اتخاذ إجراءات لحماية أنفسهم، أو مواجهة المخاطر معرفياً cope with the risk cognitively، وتجاهل آلية الحماية الموصى بها recommended protection mechanism، وهذه الشروط هي الوسائط المعرفية cognitive mediators: الشدة severity، والقابلية للتأثر vulnerability، والفائدة benefit، والتكلفة cost، والكفاءة الذاتية self efficacy، وفعالية الاستجابة response efficacy. وهذه المتغيرات سوف تؤثر في النهاية على قرار الأفراد، وبدأ استجابات التكيف (Trifiletti& et al, 2022).

استراتيجيات سلوك حماية الخصوصيَّة وفقا لنظرية دافع الحماية PMT:

ويمكن وصف سلوك حماية خصوصيَّة الأفراد بأنه إجراءات حاسوبية معينة يقوم بها الأفراد لتأمين معلوماتهم الشخصيَّة، ويضطر الأفراد إلى الاعتماد على سلوك الحماية من أجل التأقلم والحد من المخاطر والتهديد والخطر ، كما ويتم تعريف القلق بشأن خصوصيَّة المعلومات بأنه «الدرجة التي يهتم بها الفرد بشأن الممارسات التنظيمية المتعلقة بجمع واستخدام معلوماته الشخصية»، وقد تم إثبات أن مخاوف خصوصيَّة المعلومات تؤثر على سلوك حماية الخصوصيَّة لدى الأفراد في الدراسات السابقة، ويعتبر قلق خصوصيَّة المعلومات متغيرًا وسيطًا في نظرية دافع الحماية (Cozma& Muturi, 2021).

فروض النظرية وفق لسلوك حماية الخصوصية:

- درجة الخطورة:

يشير مصطلح «الخطورة المتصورة» إلى وجهة نظر الشخص القائلة: إن حدثًا مخيفًا يتسبب في إصدار حكم صارم (Chen & Hong , 2017) وتقيّم الشدة المتصورَة مدى خطورة شعور الشخص بأن التهديد سيعطل حياته، وعندما يدرك الناس العواقب غير المواتية، فإنهم سيتخذون الإجراء الموصَى به، وعلاوة على ذلك، أن زيادة دافع الفرد للانخراط في سلوك الحد من المخاطر يزداد من خلال الشدة المتصورة مما يضطر المستخدمين إلى التنازل عن خصوصيَّة المعلومات ، حيث يربطون هذه الخسارة بالمخاوف المتعلقة بخصوصيَّة المعلومات، مما سيدفعهم بشكل غير مباشر إلى استخدام تدابير حماية الخصوصيَّة في خدمات الشبكات الاجتماعية (Yao & et al , 2021).

- الضعف الملحوظ:

يصف الضعف المتصور خوف الشخص من المعاناة من عواقب غير مواتية؛ نتيجة للانخراط في سلوك محفوف بالمخاطر (Kouklakis ,2017) ووفقًا للنتائج: ارتفعت نوايا الطلاب في الانخراط في سلوك تجنب البرامج الضارة نتيجة للخطورة المتصورة. وبالتالي يتضح الضعف المتصور هو أحد المتغيرات التي تساهم في زيادة مخاوف المستهلكين بشأن خصوصيَّة المعلومات (MCMC,2014)نتيجة لذلك، ولأغراض هذا البحث، ومن المرجح أن يكون الأفراد الذين يدركون مخاطر ومخاطر فقدان خصوصيَّة المعلومات من خلال مواقع التواصل الاجتماعيّ أكثر قلقًا بشأن خصوصيتهم، مما سيدفعهم إلى استخدام إجراءات حماية الخصوصيَّة فيما بعد.

- الكفاءة الذاتية:

يتم تعريف الكفاءة الذاتية على أنها قناعة الشخص وقدرته على استخدام وسائل التواصل الاجتماعيّ مع استخدام السلوك الوقائي (Marett, McNab & Harris,2011) وتظهر بعض الدراسات أن الكفاءة الذاتية ذات تأثير كبير في قرار المستخدِم بالانخراط في سلوك خطير عبر الإنترنت. الكفاءة الذاتية هي أحد أهم العناصر التي تحفز السلوك الوقائي؛ نتيجة لذلك يشير بحثنا إلى أن الأشخاص الذين يتمتعون بالكفاءة الذاتية في استخدام SNS هم أكثر قلقًا بشأن خصوصيَّة معلوماتهم الشخصيَّة ولديهم دوافع عالية لاستخدام تقنيات سلوك حماية الخصوصية (Martin, Borah& Palmatier, 2017).

- فعالية الاستجابة:

وتعرف القدرة على التعامل مع ردود الفعل من أجل تجنب التهديد باسم: فعالية الاستجابة وتعد فعالية الاستجابة سلوكًا تنبئيًا مهمًا يحدد ما إذا كان سيتم تنفيذ ميزات الأمان على شبكاتهم أم لا، ويزيد من نوايا استخدام برامج مكافحة برامج التجسس كتقنية وقائية، ويتوقع النسخ الاحتياطي للبيانات على أجهزة الكمبيوتر الشخصية، ويتنبأ باستخدام أجهزة البرامج الضارة، وفقا لذلك يعد وجود فعالية استجابة عالية قد يساعد المستخدمين في تقليل فقدان البياناتZlatolas& et al) ,2015)

- المكافآت:

عندما يتعلق الأمر باختيار السلوك،تتعلق المكافأة بتوقع الفرد لتلقي المكافآتPalladino&et al,2017)وفقًا لبحث سابق، فإن الأشخاص الذين يحصلون على قدر كبير من المتعة والرضا من الكشف عن المعلومات الشخصيَّة هم أقل عرضة لتبني تغييرات وقائية Salleh& et al (2012,)، وبالتالي يعتقد الناس أنهم إذا كانوا مستعدين لمشاركة معلوماتهم الشخصية، فسيشعرون بأنهم أقرب إلى أصدقائهم وعائلاتهم وسيكونون راضين عن الشعور بالوحدة.

الإطار المعرفي ومصطلحات الدراسة:

تعتمد تطبيقات التَّزْيِيف الْعَمِيق على محاكاة ساخرة مزيَّفة تعتمد على تقليد الأصوات وبصمات الأصابع ثنائية الأبعاد وصور الوجه بطريقة تماثل الحقيقة، وهناك العديد من المخاطر لهذه التقنية ولعل أبرزها ما نتج عنها من تسجيلات ومقاطع فيديو وصور غير حقيقية للأشخاص وللقادة والمؤثرين لأغراض إجرامية، مما يثير مخاوف الخصوصيَّة البيومتريَّة للأشخاص الحقيقيين، وكذلك تداعيات الخصوصيَّة الرَّقميَّة حول كيفية تأثير ذلك على الأفراد والمنظمات والمجتمع في ظل التطور الرقمي في عصر الذَّكَاء الاصطناعي، وتكمن خطورة تلك التطبيقات في تأثير القوة النفسية للعناصر المرئية والأصوات ومقاطع الفيديو على المتلقي.

تقنية التعلم العميق Deep Learning: التعلم الآلي هو دراسة الخُوَارِزْمِيَّات التي تَتَعلم وتتحسن بمرور الوقت، وهي فكرة أساسية في الذَّكَاء الاصطناعي (Sayler& Harris,2020).

تقنية التَّزْيِيف الْعَمِيق Deep Fake: مزيج من «التعلم العميق» و«المزيف»، فالفيديوهات

المزيفة العميقة هي مقاطع فيديو واقعية للغاية يتم التلاعب بها رقميًا لتصوير أشخاص يقولون ويفعلون أشياء لم تحدث بالفعل (Tesfagergish &Dzikien, 2021)، تعتمد تقنية التَّزْييف الْعَمِيق على الشبكات العصبية التي تحلل مجموعات كبيرة من البيانات الرَّقميَّة بشكل آلي يتم من خلاله تقليد تعبيرات وجه الشخص وسلوكياته وصوته وتصرفاته(Sayler& Harris, 2020)، تستخدم تقنية التَّزْييف الْعَمِيق تقنية رسم خرائط الوجه والذكاء الْإِصْطِنَاعِيّ لاستبدال وجه شخص في مقطع فيديو بوجه شخص آخر(Visvikis& et al, 2019).

التزييف العميق: هو مقطع فيديو أو صورة يتم التلاعب بها بالذكاء الْإِصْطِنَاعِيّ لتجعلك تصدق شيئًا غير حقيقي. بينما يستخدم معظم الأشخاص تقنية التَّزْييف الْعَمِيق في أغراض إيجابية، يستخدمها البعض لنشر المعلومات المضللة على نطاق أوسع وأسرع عبر وسائل التواصل الاجتماعيّ، على سبيل المثال يمكن أن يخلق أشخاصًا غير موجودين بالفعل أو يُظهر أشخاصًا حقيقيين يفعلون ويقولون أشياء لم يفعلوها أو يقولوها (Laishram& Jung, 2021).

البيانات الشخصيَّة وفق قانون حماية البيانات الشخصيَّة في مادة رقم (1) أنها: أية بيانات متعلقة بشخص طبيعي محدد، أو يمكن تحديده، بشكل مباشر أو غير مباشر عن طريق الربط بينها وبين بيانات أخرى كالاسم، أو الصوت، أو الصورة، أو رقم تعريفي، أو محدد للهوية عبر الانترنت، أو أية بيانات تحدد الهُوِيَّة النفسية، أو الصحية، أو الاقتصادية، أو الثقافية (Fletcher, 2018) وكذلك لا يجوز جمع البيانات الشخصيَّة أو معالجتها أو الإفصاح أو الافشاء عنها بأية وسيلة من الوسائل إلا بموافقة صريحة من الشخص المعني بالبيانات أو في الأحوال المصرح بها قانونا.

البيانات الرَّقميَّة: هي بيانات يتم جمع عدد ضخم منها من مستخدمي وزائري المواقع الالكترونية، والتي يمكن من خلالها تحليل وترتيب توقع نمط المستخدم وتفاعله مع الإنترنت، بحيث تمثل تلك المعلومات مكسبا اقتصاديا كبيرا لشركات الإعلان والتسويق بما يسمح بتسريب البيانات الشخصيَّة عبر شبكة الإنترنت على غير رغبة المستخدم أو دون معرفته لتأثيراتها، فعادة المواقع الالكترونيَّة عند التسجيل عليها وضع نوعين من السياسات على موقعها: سياسة الخصوصيَّة Privacy Policy و Usage Policyسياسة الاستخدام (Hasan & Salah, 2019).

سياسة الخصوصيَّة: هي ماهية المعلومات الشخصيَّة التي يتم جمعها، وكيفية استخدام الموقع للبيانات المجمعة، ويتم توضيح كل أو بعض الطرق التي يتم بها جمع وتخزين بيانات المستخدم، أو حفظها بسرية، أو استخدمها، أو الإفصاح عنها والتحكم بها، أو تداولها مع طرف ثالث .

سياسة الاستخدام: قواعد استخدم الموقع وما هو مسموح به، وما تعتبره إدارة الموقع انتهاكا يُلزم وقف حساب المستخدم أو إلغائه (Yang& Tsai, 2020).

الخصوصيَّة الرَّقميَّة البيومتريَّة: هي الخصوصيَّة البيولوجية أو الفسيولوجية الرَّقميَّة عبر المواقع والتطبيقات الإلكترونيَّة مثل: بصمات الأصابع، وبنية الوجه، وأنماط القزحية أو الشبكية، والتعرف الصوتي التي يتم قياسها وتقييمها لتحديد الهوية(Schneider, Fürsich& Werner, 2011).

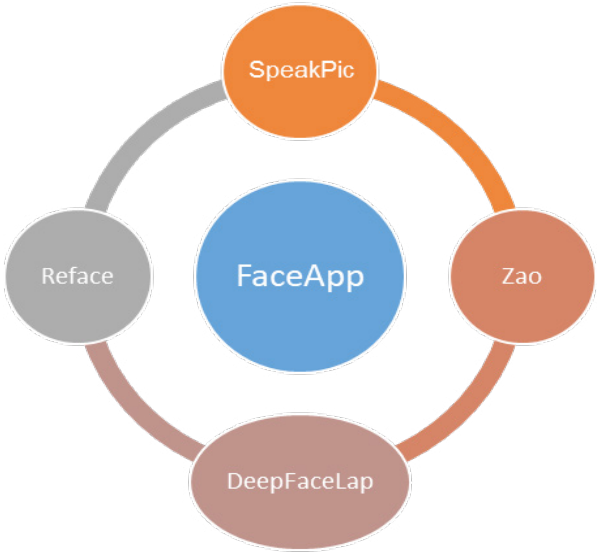
بروتوكول الإنترنت (Internet Protocol) (IP address): هو بروتوكول أو مرسوم بكيفية تبادل المعلومات بين طرفين على شبكة الإنترنت بحيث لا يتشابه أي عنوان للبروتوكول مع غيره

على الإطلاق (Dong& Zheng, 2020).

برتوكول التطبيقات: هو مجموعةٌ من القواعد الإلكترونيَّة المقبولة والمطبقة بشكلٍ متبادلٍ على طرفي التطبيق (المصمم والمستخدم) من أجل التبادل السليم للمعلومات مع الالتزام بالقواعد الاستخدام وقواعد خصوصيَّة المستخدم (Komkova & Kulikova, 2020).

آلية جمع البيانات الرَّقميَّة البيومتريَّة: تعرف البيانات البيومتريَّة بأنها السمات الحيوية الفريدة الخاصة بكل مستخدم على حدة، وتبدأ عملية تجميع البيانات الرَّقميَّة البيومتريَّة منذ اللحظة الأولى التي يقوم المستخدم بتصفح أحد التطبيقات والمواقع الإلكترونيَّة بواسطة بعض العناصر التي تحتوي عليها صفحة الإنترنت مثل بصمة الوجه، وبصمة الأصابع، وبصمة الصوت,LEE& Al Khaldi (2020) ، حيث يتم كل ذلك بشكل رقمي، وعن طريق تتبع عنوان البروتوكول يتم الوصول إلى البيانات الشخصيَّة الرَّقميَّة وربطها بالبيانات البيومتريَّة للمستخدمين، والتعرف أيضا على موقع الجهاز الذي يقوم بعملية التصفح على الإنترنت (Chowdhury& Lubna, 2020).

تطبيقات التزييف العميق



شكل رقم (1) يوضح أسماء تطبيقات التزييف العميق.

- **كما نجد ما ذكره موقع (knowledgenile.com ,2020) عن تطبيقات التزييف العميق:**

- **FaceApp** يسمح للمستخدمين بتحويل صورهم باستخدام AI، ويوفر مجموعة متنوعة من التأثيرات والخلفيات والمرشحات التي يمكنك استخدامها لتغيير مظهرك.

- **Zao** هو تطبيق لمبادلة الوجه انتشر منذ وقت ليس بعيدا، ولا يسمح هذا فقط لشخصين بتبديل الوجوه، بل يضيف أيضًا وجهك إلى أي فيديو.

- **Reface** هو أحد أشهر تطبيقات deepfake في العالم، إنه يركب وجهك على الصور وصور GIF باستخدام AI مبادلة الوجه.

- **SpeakPic** يتيح للمستخدمين جعل صورهم تتحدث باستخدام الذَّكَاء الاصطناعي، عن طريق تسجيل أو كتابة أي نص وسيقوم البرنامج بترديد ما تقول.

- **DeepFaceLab** هي الشركة الرائدة في مجال برامج التزييف العميق، ويمكن لنظام deepfake تبديل الوجوه في الفيديو أو الصور وغير ذلك الكثير.

- **FakeApp** هو برنامج شائع آخر للتزييف العميق يسمح للمستخدمين بتحميل الوجوه في مقاطع الفيديو الخاصة بهم أو مع شخص آخر.

- **Reflect** يعد أحد أكثر تطبيقات تبديل الوجه، حيث يقوم باستخدام أدوات الفيديو والتماثيل واللوحات وما إلى ذلك.

- **Deepfakes Web** يستخدم خُوَارِزْمِيَّة التعلم الآلي لمبادلة موضوع مقطع فيديو بآخر.

- **Instagram DeepFake Bot** يعمل كحساب يمكن لأي شخص استخدامه لإنشاء صور مزيفة.

- **Deepfake Studio** يتيح تبديل الوجوه في مشهد الفيلم ومقاطع الفيديو الموسيقية وغيرها، وهناك احتمالات لا حصر لها لمبادلة الوجه لأنها تستخدم التعلم العميق مع مجموعة من الجوانب.

شكل (2) يوضح التَّزْيِيف الْعَمِيق، فيعرض الصف الأول إطارات الفيديو الأصلية، بينما يعرض الصف الثاني إطارات الفيديو التي تم إنشاؤها باستخدام تقنية التزييف العميق.

الإجراءات المنهجية للدراسة:

- **نـوع ومنهـج الدراسـة:** تنتمي هذه الدراسة إلى الدراسات الوصفية التي تهدف إلى وصف خصائص ظاهرة أو مجموعة معينة محل الدراسة، من خلال مجموعة من التساؤلات أو الفروض تمكنه من إجراء الوصف، وتعتمد الدراسة على منهج المسح بالعينة كأحد الأساليب البحثية المستخدمة في البحوث الوصفية، حيث تستخدم الدراسة المسح الوصفي الذي يصف سلوك العينة، فهو يساعد في التعرف على اتجاهات المبحوثين وآرائهم ، ويهدف المسح المستخدم في الدراسة إلى مسح مستخدمي تطبيقات التزييف العميق من طلبة الجامعات المصرية ووصف سلوك حماية الخصوصية البيومترية لديهم .

مجتمع وعينة الدراسة:

- **مجتمـع الدراسـة:** يتمثل في الجامعات المصرية (الحكومية –الخاصة) ،(الريف –الحضر)، (الكليات العلمية –الكليات الأدبية).
- **عينة البحث الاستطلاعية:** اعتمدت الباحثة في التحقق من الخصائص السيكومترية (الصدق، والثبات) لمقياس سلوك الحماية البيومترية لدى طلبة الجامعة مستخدمي تطبيقات التزييف العميق على عينة من طلبة المرحلة الجامعية بالجامعات المصرية ، تكونت من (280) طالبا وطالبة في عدة جامعات مختلفة من الفرقة الأولى حتى الرابعة، ومأخوذة من الكليات العلمية والأدبية المختلفة.
- **عينة البحث الأساسية:**

تكونت عينة البحث الأولية من عينة عشوائية (390): (219 ذكورا ، 171 إناثا) من طلبة المرحلة الجامعية (300) من مستخدمي تطبيقات التزييف العميق، و(90) من غير مستخدمي تطبيقات التزييف العميق)، وحيث إن البحث يستهدف فئة الطلبة مستخدمي تطبيقات التزييف العميق؛ فقد تحددت عينة الدراسة النهائية في (300) (173: بنسبة 57.7 % من الذكور، 127 بنسبة: 42.3 % من الإناث) من طلبة المراحل الجامعية في سنوات دراسية مختلفة، والعينة مأخوذة بشكل عشوائيّ من (8) جامعات مصرية حكوميَّة وخاصة متنوعة، ومن كليات علميَّة وأدبيَّة مختلفة، ومن بيئات ريفية وحضرية منتسبة إلى عدة محافظات مختلفة، وقد تراوحت الأعمار الزمنية لأفراد عينة الدراسة بين (19.2 إلى 28.4) سنة بمتوسط عمر زمني (21.7) سنة، وانحراف معياري (1.06)، وجميع أفراد العينة النهائية من مستخدمي الهواتف الذكية: إما بنظام Android، أو بنظام IOS .

أدوات جمع البيانات: مقياس دافع حماية الخصوصيَّة البيومتريَّة وفقا لنظرية دافع الحماية PMT الذي قامت الباحثة بإعداده .

مقياس سلوك الحماية البيومترية لدى مستخدمي تطبيقات التزييف العميق عبر الإنترنت:

جدول رقم (1) الأبعاد والمفردات لمقياس سلوك الحماية البيومترية لدى مستخدمي تطبيقات التزييف العميق

م	الأبعاد	عدد المفردات	أرقام المفردات
1	الشدة المدركة	16	16-1
2	القابلية للتأثير المدركة	14	30 - 17
3	الكفاءة الذاتية	13	43 - 31
4	فعالية الاستجابة	11	54 - 44
5	المكافئات	8	62 - 55
6	الاستراتيجيات المستخدمة	9	71 - 63
الإجمالي		71 مفردة	

جدول رقم (2) أرقام المفردات السلبية في مقياس سلوك الحماية البيومترية لدى مستخدمي تطبيقات التزييف العميق

المفردات السلبية	7 ، 8 ، 9 ، 11 ، 12 ، 26 ، 62 ، 63 ، 64 ، 65 ، 66 ، 67 ، 68 ، 69 ، 70 ، 71

إجراءات التحقق من صدق المقياس:

(1)صدق المحكمين:

حيث تم عرض المقياس على مجموعة من الأساتذة المتخصصين في التربية وعلم النفس، وذلك لتحديد الصدق الظاهري لمقياس سلوك الحماية البيومتريَّة، ومدى ملاءمة صياغة المفردات لخصائص عينة الدراسة، وقد بلغت نسبة اتفاق المحكمين على مفردات المقياس ككل (96.2 %) وهي نسبة مرتفعة تدل على صلاحية مفردات المقياس لقياس الجوانب المختلفة لسلوك الحماية البيومترية، هذا وقد شملت التعديلات التي أدخلت على المقياس وفقا لآراء المحكمين: (أ) **تعديل صياغة بعض الألفاظ والعبارات، (ب) الموازنة بين عدد المفردات التي تقيس كل بُعد، (ج) تعديل معيار التقييم من ثلاثي إلى خماسي.**

(2) الاتساق الداخلي:

تحققت الباحثة من الاتساق الداخلي لمقياس سلوك الحماية البيومتريَّة من خلال حساب قيمة معامل ارتباط بيرسون بين درجة كل مفردة والدرجة الكلية على مقياس سلوك الحماية البيومتريَّة

بعد تطبيق المقياس لدى أفرد العينة الاستطلاعية (ن = 280)، وبإجراء المعالجة باستخدام برنامج الحزم الإحصائية SPSS (إصدار 26) جاءت جميع قيم معاملات الارتباط تتراوح بين (0.389 إلى 0.713) وجميعها دالة إحصائياً عند مستوى دلالة (0.01).، بما يشير إلى قوة ارتباط كل مفردة بالدرجة الكلية للمقياس.

(3) التحليل العاملي:

للتحقق من البنية العاملية لمقياس سلوك الحماية البيومتريَّة قامت الباحثة بإجراء التحليل العاملي لمفردات المقياس بناء على ما أسفرت عنه نتائج الاتساق الداخلي للمفردات في الإجراء السابق، وبإدراج جميع مفردات المقياس في التحليل العاملي؛ حيث استخدمت الباحثة أسلوب التحليل العاملي الاستكشافي Exploratory Factor analysis لمفردات المقياس بهدف الكشف عن البنية العاملية Factorial structure للمقياس وتحديد المكونات العاملية المتمايزة له، حيث طُبق المقياس على عينة التقنين التي تكونت من (280) طالبا من طلبة المرحلة الجامعية، وقد بلغ عدد المفردات الأولية للمقياس المدرجة في التحليل العاملي الأولي (71) مفردة، وتم الاعتماد في التحليل العاملي الاستكشافي لتلك المفردات على طريقة المكونات الأساسية Principle Component لهوتلينج والتدوير المائل بطريقة Direct Oblimin، والاعتماد على محك كايزر Kaiser وأن لا تقل قيمة الجذر الكامن (القيمة المميزة) Eigenvalue عن الواحد الصحيح، كما تم استبعاد المفردات ذات التشبعات الأقل من (0.3)، وقد أسفرت نتائج التحليل – باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعيَّة SPSS (إصدار 26) – عن النتائج الآتية:

1. بلغت قيمة مقياس اختبار كفاية العينة Kaiser–Meyer–Olkin Measure(0.958) وهي قيمة مرتفعة تشير لصلاحية عينة التقنين لإجراء التحليل العاملي.
2. تراوحت قيم الشيوع لجميع مفردات المقياس بين (0.514 إلى 0.667).
3. ظهرت (6) عوامل تفسر جميعها نسبة (58.89 %) من قيمة التباين الكلي للمقياس، ويوضح الجدول رقم (3) ملخصا لأهم النتائج التي أسفر عنها التحليل العاملي لمفردات المقياس.

جدول رقم (3) ملخص نتائج التحليل العاملي لمقياس سلوك الحماية البيومترية.

العوامل	عدد المفردات التي تشبعت على العامل	مسميات الأبعاد	أرقام المفردات	الجذر الكامن	نسبة التباين المفسرة %	نسبة التباين التراكمية %
الأول	16	الشدة المدركة	1–16	10.80	% 15.21	% 15.21
الثاني	14	القابلية للتأثير المدركة	17 – 30	8.27	% 11.65	% 26.86
الثالث	13	الكفاءة الذاتية	31 – 43	7.97	% 11.22	% 38.09
الرابع	11	فعالية الاستجابة	44 – 54	6.31	% 8.89	% 46.98

الخامس	8	المكافآت	55 - 62	4.46	% 6.28	% 53.26
السادس	9	الاستراتيجيات المستخدمة	63 - 71	3.99	% 5.62	% 58.89

بهذا يتبين من النتائج الموضحة بالجدول رقم (3) إلى أن التحليل العاملي قد أسفر عن وجود ستة عوامل تم تسميتها على النحو الآتي وفقا لتعريف كل بُعد والمظاهر السلوكية الدالة عليه: (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت، الإستراتيجيات المستخدمة)، وأنها تفسر جميعها نسبة (58.89) من التباين الكلي بين الأفراد في سلوك الحماية البيومترية.

ثانياً: إجراءات التحقق من ثبات المقياس:

تحققت الباحثة من ثبات مقياس سلوك الحماية البيومتريَّة المعد من خلال تطبيقه على عينة التقنين (ن = 280) باستخدام ثلاث طرق تمثلت في: (أ) إعادة التطبيق، (ب) التجزئة النصفية (معادلة سبيرمان – براون)، (ج) معامل ألفا – كرونباخ، وفيما يلي توضيح للإجراءات المتبعة في كل منهم:

(أ) طريقة إعادة التطبيق Test Retest Method: حيث طُبق المقياس على جزء من عينة التقنين بلغ (ن = 85) مرتين بفاصل زمني (18) يوماً على نفس العينة، وفي نفس الظروف تقريبا، وبحساب معامل الارتباط (معامل الثبات) بين التطبيقين الأول والثاني للأبعاد الفرعية الستة والدرجة الكلية للمقياس، جاءت نتائج قيم معاملات الثبات للأبعاد الستة (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت، الإستراتيجيات المستخدمة) والدرجة الكلية تتراوح بين (0.727 إلى 0.891) وجميعها قيم مرتفعة تشير إلى ثبات مرتفع لجميع الأبعاد الفرعية والدرجة الكلية للمقياس، مما يشير إلى أن المقياس يتسم بدرجة عالية من الثبات.

بهذا تشير جميع إجراءات التحقق من صدق وثبات مقياس سلوك الحماية البيومتريَّة إلى أن المقياس المعد يتسم بدرجة عالية من الصدق والثبات، مما يشير إلى إمكانية الاعتماد عليه في قياس سلوك الحماية البيومتريَّة لدى أفرد عينة الدراسة.

ما هي درجة توافر سلوكيات دافع الحماية البيومترية لدى طلبة الجامعات المصرية مستخدمي تطبيقات التزييف العميق ؟

وللإجابة على هذا السؤال قامت الباحثة بإجراء الخطوات الآتية :

(1) تحديد معيار ومدى كل فئة وفقا لمقياس ليكرت الخماسي ودرجة التقييم .

(2) تحديد قيمة التكرارات والنسبة المئوية لبدائل الاستجابات الخمسة على كل مفردة لدى أفراد عينة الدراسة الكلية ن = 300 .

(3) حساب قيمة المتوسط الحسابي والانحراف المعياري والمستوى لكل مفردة لدى أفراد عينة الدراسة الكلية ن = 300 .

(4) حساب قيمة المتوسط المرجح والإنحراف المعياري الكلي لكل محور .

جدول (4) معيار ومدى تقييم فئات المقياس الخماسي

ضعيفة جدا	ضعيفة	متوسطة	مرتفعة	مرتفعة جدا
من 1 – 1.80	من 1.81 – 2.60	من 2.61 – 3.40	من 3.41 – 4.20	من 4.21 – 5

جدول (5) التكرارات والنسب المئوية والمتوسط والانحراف المعياري والمستوى لاستجابات طلبة الجامعة مستخدمي تطبيقات التزييف العميق (ن = 300)

البعد الأول : الشدة المدركة perceived severity :

م	المفردة		النسب المئوية للاستجابات ن = 300					المتوسط	الانحراف المعياري	المستوى
			غير موافق تماماً	غير موافق	إلى حد ما	موافق	موافق تماماً			
1	يعد انتهاك المعلومات الشخصية لي في استخدام تطبيقات الانترنت مشكلة خطيرة بالنسبة لي .	العدد	149	35	43	34	39	2.6	1.48	ضعيف
		%	49.7	11.7	14.3	11.3	13			
2	اذا توصل الآخرون الى معلوماتي الشخصية بأسلوب غير صحيح ، فسوف يؤثر ذلك على سمعتي بدرجة كبيرة .	العدد	37	125	71	35	32	2.67	1.16	متوسط
		%	12.3	41.7	23.7	11.7	10.7			
3	إذا رأى الآخرون معلوماتي وصوري الشخصية عبر تطبيقات الإنترنت دون إذن مني ، فقد يحرجني ذلك بشدة .	العدد	40	76	111	38	35	2.84	1.16	متوسط
		%	13.3	25.3	37	12.7	11.7			
4	إذا سُرقت هويتي الشخصية عبر الانترنت فسيكون لذلك عواقب سلبية وخيمة على حياتي الشخصية .	العدد	49	65	69	70	47	3	1.31	متوسط
		%	16.3	21.7	23	23.3	15.7			
5	إذا سُرقت هويتي الشخصية عبر الانترنت فسيكون ذلك أمر مزعج لي تماماً	العدد	40	63	85	50	62	3.10	1.31	متوسط
		%	13.3	21	28.3	16.7	20.7			
6	قد أصيب بالضرر إذا تم وصول الآخرين إلى تفاصيل هويتي الشخصية .	العدد	43	97	76	47	37	2.79	1.22	متوسط
		%	14.3	32.3	25.3	15.7	12.3			

7	تطبيقات التزييف العميق Deepfake عبر الانترنت هي تطبيقات آمنة تعزز العلاقات والتواصل مع الآخرين .	العدد	28	23	95	82	72	3.49	1.20	مرتفع (سالب)
		%	9.3	7.7	31.7	27.3	24			
8	تطبيقات التزييف العميق عبر الانترنت هي تطبيقات جديرة بالثقة .	العدد	27	27	72	110	64	3.52	1.18	مرتفع (سالب)
		%	9	9	24	36.7	21.3			
9	تطبيقات التزييف العميق عبر الانترنت تتعامل مع المعلومات الشخصية بطريقة سرية احترافية .	العدد	29	22	89	95	65	3.48	1.18	مرتفع (سالب)
		%	9.7	7.3	29.7	31.7	21.7			
10	أشعر بالقلق أو التوتر عندما أفكر في إمكانية سرقة الخصوصية البيومترية أو الأكونت الخاص بي .	العدد	46	81	91	44	38	2.82	1.22	متوسط
		%	15.3	27	30.3	14.7	12.7			
11	لست في حاجة إلى إستخدام اجراءات حماية الخصوصية البيومترية .	العدد	30	34	96	79	61	3.36	1.21	متوسط
		%	10	11.3	32	26.3	20.3			
12	لا داعي للقلق بشأن التعدي على الخصوصية البيرمترية لأن فرصة سرقة هويتي تكاد تكون معدومة .	العدد	37	40	75	93	55	3.30	1.26	متوسط
		%	12.3	13.3	25	31	18.3			
13	قد تستخدم المعلومات الشخصية التي أوافق عليها في تطبيقات التزييف العميق بشكل سيء .	العدد	56	72	93	44	35	2.77	1.24	متوسط
		%	18.7	24	31	14.7	11.7			
14	قد يكون جهاز الكمبيوتر الخاص بي مخترق ببرامج تجسس بسبب استخدامي لتطبيقات التزييف العميق	العدد	53	77	101	36	33	2.73	1.20	متوسط
		%	17.7	25.7	33.7	12	11			
15	يعد نشر معلومات شخصية عبر بعض تطبيقات الانترنت أمرًا محفوفًا بالمخاطر	العدد	48	81	90	43	38	2.81	1.23	متوسط
		%	16	27	30	14.3	12.7			
16	أنا حريص على المعلومات أو الصور التي أنشرها عبر تطبيقات التزييف العميق	العدد	75	81	87	39	36	2.72	1.25	متوسط
		%	19	27	29	13	12			
	المتوسط المرجح والإنحراف المعياري للمحور الأول كلياً							**2.97**	**0.501**	

البعد الثاني : القابلية للتأثير المدركة perceived vulnerability

م	المفردة		النسب المئوية للاستجابات ن = 300					المتوسط	الانحراف المعياري	المستوى
			غير موافق تماماً	غير موافق	إلى حد ما	موافق	موافق تماماً			
17	من المتوقع أن تستخدم معلوماتي الشخصية بشكل غير لائق نتيجة استخدامي لتطبيقات التزييف العميق عبر الإنترنت .	العدد	52	84	85	46	33	2.75	1.22	متوسط
		%	17.3	28	28.3	15.3	11			
18	من المتوقع أن تؤدي المعلومات التي أشاركها في تطبيقات الإنترنت إلى انتهاك الخصوصية البيومترية لدي .	العدد	52	84	91	35	38	2.74	1.23	متوسط
		%	17.3	28	30.3	11.7	12.7			
19	يمكن للآخرون الوصول إلى المعلومات التي أشاركها في الشبكات الاجتماعية عبر الإنترنت دون علمي بذلك .	العدد	52	78	84	52	34	2.79	1.24	متوسط
		%	17.3	26	28	17.3	11.3			
20	المعلومات التي أوافق عليها في تطبيقات التزييف العميق عبر الإنترنت يمكن أن يراها الآخرون دون إذني أو تصريح مني .	العدد	47	66	106	42	39	2.87	1.22	متوسط
		%	15.7	22	35.3	14	13			
21	من المتوقع أن تسرق هويتي الشخصية أو يتعدى على الخصوصية البيومترية لي عبر بعض تطبيقات الانترنت التي استخدمها.	العدد	42	87	79	54	38	2.86	1.23	متوسط
		%	14	29	26.3	18	12.7			
22	من المتوقع أن يكون الأكونت الخاص بي مخترق من قبل الآخرين .	العدد	44	87	98	34	37	2.78	1.19	متوسط
		%	14.7	29	32.7	11.3	12.3			
23	من المتوقع أن تكون هويتي الشخصية مسروقة ، أو يمكن سرقتها .	العدد	43	89	84	49	35	2.81	1.21	متوسط
		%	14.3	29.7	28	16.3	11.7			
24	سيكون هناك احتمال كبير للخسائر المترتبة على استخدامي لتطبيقات التزييف العميق .	العدد	54	80	89	39	38	2.76	1.25	متوسط
		%	18	26.7	29.7	13	12.7			
25	قد يترتب على استخدامي لتطبيقات التزييف العميق العديد من المشكلات المستقبلية غير المتوقعة .	العدد	50	78	98	37	37	2.78	1.22	متوسط
		%	16.7	26	32.7	12.3	12.3			

26	أشعر بالأمان والراحة عند استخدام تطبيقات التزييف العميق .	العدد	29	33	93	86	59	3.38	1.19	مرتفع (سالب)
		%	9.7	11	31	28.7	19.7			
27	تشكل استخدامي لتطبيقات التزييف العميق تهديدًا لخصوصيتي البيومترية .	العدد	45	86	86	48	35	2.81	1.21	متوسط
		%	15	28.7	28.7	16	11.7			
28	قد يؤدي استخدامي لتطبيقات التزييف العميق إلى تعريض أمن معلوماتي للخطر	العدد	44	81	82	53	40	2.88	1.24	متوسط
		%	14.7	27	27.3	17.7	13.3			
29	قد تستخدم المعلومات أو الصورة التي اوافق عليها أثناء استخدامي لتطبيقات التزييف العميق من قبل المتسللين hackers لسرقة المعلومات مني .	العدد	39	79	91	53	38	2.91	1.20	متوسط
		%	13	26.3	30.3	17.7	12.7			
30	يمكن للآخرين استغلال استخدامي لتطبيقات التزييف العميق في انشاء رسائل وفيديوهات مفتعلة لابتذاذي بها .	العدد	48	87	95	31	39	2.75	1.22	متوسط
		%	16	29	31.7	10.3	13			
	المتوسط المرجح والإنحراف المعياري للبعد الثاني كلياً							2.84	0.819	

البعد الثالث : الكفاءة الذاتية Self-efficacy

م	المفردة		النسب المئوية للاستجابات ن = 300					المتوسط	الوزن النسبي	المستوى
			غير موافق تماماً	غير موافق	إلى حد ما	موافق	موافق تماماً			
31	أعتقد أنني قادر على استخدام إعدادات الخصوصية عبر تطبيقات الانترنت مثل تطبيقات التزييف العميق .	العدد	102	78	66	22	32	2.35	1.30	ضعيف
		%	34	26	22	7.3	10.7			
32	أستطيع التحكم في الإعدادت شديدة الخصوصية أثناء استخدامي لتطبيقات التزييف العميق .	العدد	31	96	110	34	29	2.78	1.09	متوسط
		%	10.3	32	36.7	11.3	9.7			
33	أثق في قدرتي على استخدامي لتطبيقات التزييف العميق بحرفية وأمان .	العدد	36	84	105	43	32	2.84	1.14	متوسط
		%	12	28	35	14.3	10.7			

34	يسهل عليّ استخدام برنامج الأمان Security software كأحد اجراءات حماية الهوية الشخصية .	العدد	33	72	96	61	38	3	1.18	متوسط
		%	11	24	32	20.3	12.7			
35	يعد برنامج الأمان Security software أحد أفضل البرامج الملائمة لحماية الهوية الشخصية .	العدد	38	72	103	52	35	2.91	1.17	متوسط
		%	12.7	24	34.3	17.3	11.7			
36	لدي القدرة على استخدام برنامج الأمان Security software بأقل جهد ممكن .	العدد	35	91	108	38	28	2.78	1.10	متوسط
		%	11.7	30.3	36	12.7	9.3			
37	يسهل عليّ القيام بفحص الائتمان كأحد إجراءات حماية الهوية أو الخصوصية البيومترية .	العدد	49	85	101	36	29	2.70	1.16	متوسط
		%	16.3	28.3	33.7	12	9.7			
38	لدي القدرة على إجراء فحص الائتمان بأقل جهد.	العدد	59	93	83	35	30	2.61	1.21	متوسط
		%	19.7	31	27.7	11.7	10			
39	لدي القدرة على اكتشاف هجمات التصيد الاحتيالي التي تحاول إعادة توجيهي إلى مواقع ويب مزيفة.	العدد	45	90	103	34	28	2.70	1.14	متوسط
		%	15	30	34.3	11.3	9.3			
40	لدي القدرة على اكتشاف الرسائل العشوائي المزعجة social spams ، والتي قد تبدو أنها رسائل من أصدقائي.	العدد	48	84	99	39	30	2.73	1.17	متوسط
		%	16	28	33	13	10			
41	أستطيع التحكم بسهولة في إعدادات الخصوصية للتحكم في الوصول إلى معلوماتي الشخصية أثناء استخدامي لتطبيقات التزييف العميق .	العدد	38	82	93	49	38	2.89	1.20	متوسط
		%	12.7	27.3	31	16.3	12.7			
42	لدي القدرة على تغيير إعدادات الخصوصية في استخدام تطبيقات الانترنت لضبط كيفية مشاركة المعلومات مع الآخرين .	العدد	55	75	91	42	37	2.77	1.25	متوسط
		%	18.3	25	30.3	14	12.3			
43	أصبح استخدام إعدادات الخصوصية الافتراضية أثناء استخدامي أمرا تلقائيًا لي	العدد	39	84	93	45	39	2.87	1.20	متوسط
		%	13	28	31	15	13			
	المتوسط المرجح والإنحراف المعياري للبعد الثالث كلياً							2.76	0.861	

البعد الرابع : فعالية الاستجابة Response efficacy :

م	المفردة		النسب المئوية للاستجابات ن = 300					المتوسط	الوزن النسبي	المستوى
			غير موافق تماماً	غير موافق	إلى حد ما	موافق	موافق تماماً			
44	استخدام إعدادات الخصوصية يعمل على منع انتهاك الخصوصية البيومترية .	العدد	45	74	111	38	32	2.79	1.16	متوسط
		%	15	24.7	37	12.7	10.7			
45	استخدام إعدادات الخصوصية يعد أمرا فعالاً في منع انتهاك الخصوصية البيومترية .	العدد	40	84	105	40	31	2.79	1.15	متوسط
		%	13.3	28	35	13.3	10.3			
46	إذا استخدمت إعدادات الخصوصية فأنا أقل عرضة لانتهاك خصوصيتي البيومترية .	العدد	45	79	99	46	31	2.80	1.18	متوسط
		%	15	26.3	33	15.3	10.3			
47	يعد استخدام برامج الأمان security software أحد الإجراءات الجيدة في حماية الهوية من السرقة .	العدد	46	77	103	45	29	2.78	1.16	متوسط
		%	15.3	25.7	34.3	15	9.7			
48	إذا استخدمت برنامج أمان ، فأنا أقل عرضة لسرقة هويتي .	العدد	31	81	101	52	35	2.93	1.15	متوسط
		%	10.3	27	33.7	17.3	11.7			
49	يعد إجراء فحص الائتمان a credit check فعالا في منع سرقة الهوية البيومترية	العدد	38	75	98	57	32	2.90	1.17	متوسط
		%	12.7	25	32.7	19	10.7			
50	إذا قمت بإجراء فحص ائتماني فمن الصعب جدا أن تتم سرقة هويتي البيومترية	العدد	40	88	92	47	33	2.82	1.18	متوسط
		%	13.3	29.3	30.7	15.7	11			
51	يمكنني من خلال استخدام إعدادات الخصوصية تقييد المعلومات السرية للأشخاص المصرح لهم.	العدد	38	81	102	46	33	2.85	1.16	متوسط
		%	12.7	27	34	15.3	11			
52	ان التحقق من سياسات التطبيق المستخدم يضمن لي أنني أمنح حق الوصول لمعلوماتي للجهات والأشخاص الموثوق بها فقط .	العدد	42	72	98	60	28	2.87	1.16	متوسط
		%	14	24	32.7	20	9.3			

53	تؤدي مراجعة حساسية المعلومات قبل القبول والنشر عبر تطبيقات الإنترنت إلى منع الإفصاح غير المناسب للمعلومات الشخصية	العدد	47	81	100	44	28	2.75	1.16	متوسط
		%	15.7	27	33.3	14.7	9.3			
54	تحكمي بدقة في مقدار المعلومات الشخصية التي اسمح بها أثناء استخدامي لتطبيقات التزييف العميق يجعلني مطمئنا لاستخدامه .	العدد	47	93	90	42	28	2.70	1.16	متوسط
		%	15.7	31	30	14	9.3			
المتوسط المرجح والإنحراف المعياري للبعد الرابع كلياً								2.81	0.875	

البعد الخامس : المكافئات Rewards

م	المفردة		النسب المئوية للاستجابات ن = 300					المتوسط	الوزن النسبي	المستوى
			غير موافق تماماً	غير موافق	إلى حد ما	موافق	موافق تماماً			
55	يسهل عَليّ ضبط إعدادات الخصوصية privacy settings لتطبيقات التزييف العميق للتحكم في الاشخاص التي يمكنها الوصول إلى معلوماتي .	العدد	104	76	53	33	34	2.39	1.35	ضعيف
		%	34.7	25.3	17.7	11	11.3			
56	يسهل عَليّ تحديد ما إذا كان يجب نشر جزء من المعلومات الخاصة بي عبر الإنترنت .	العدد	35	100	99	35	31	2.76	1.12	متوسط
		%	11.7	33.3	33	11.7	10.3			
57	إذا احسنت استخدمت اعدادات التطبيقات عبر الإنترنت ، فسأزيد من فرصة تطوير أفكار أو منتجات أو خدمات مبتكرة.	العدد	43	69	98	59	31	2.89	1.18	متوسط
		%	14.3	23	32.7	19.7	10.3			
58	استخدامي للتطبيقات التزييف العميق عبر الإنترنت يُمكّنني من تطوير مسيرتي المهنية.	العدد	41	77	97	51	34	2.87	1.18	متوسط
		%	13.7	25.7	32.3	17	11.3			
59	من المفيد أن أتناقش مع الأصدقاء والآخرين في القضايا الأمنية المتعلقة بتطبيقات التزييف العميق	العدد	49	69	93	49	40	2.87	1.25	متوسط
		%	16.3	23	31	16.3	13.3			
60	أهم شيء بالنسبة لي أثناء استخدام تطبيقات الانترنت أن أحافظ على خصوصيتي البيومترية	العدد	41	84	89	48	38	2.86	1.21	متوسط
		%	13.7	28	29.7	16	12.7			

م			غير موافق تماماً	غير موافق	إلى حد ما	موافق	موافق تماماً	المتوسط	الوزن النسبي	المستوى
			النسب المئوية للاستجابات ن = 300							
61	يتيح لي الاستخدام المقنن والآمن لتطبيقات التزييف العميق إقامة علاقات جيدة مع أصدقائي	العدد	60	85	92	38	25	2.61	1.18	متوسط
		%	20	28.3	30.7	12.7	8.3			
62	أشعر أحيانًا أنه من غير المجدي محاولة حماية خصوصيتي البيومترية	العدد	25	35	86	105	49	3.39	1.14	متوسط (سالب)
		%	8.3	11.7	28.7	35	16.3			
	المتوسط المرجح والإنحراف المعياري للبعد الخامس كلياً							2.82	0.729	

البعد السادس: الاستراتيجيات حماية الخصوصية

م	المفردة		غير موافق تماماً	غير موافق	إلى حد ما	موافق	موافق تماماً	المتوسط	الوزن النسبي	المستوى
			النسب المئوية للاستجابات ن = 300							
63	أوافق على تحديد الموقع الجغرافي لي وتشغيل ال GPS أثناء استخدام التطبيق	العدد	32	37	76	87	68	3.41	1.26	مرتفع (سالب)
		%	10.7	12.3	25.3	29	22.7			
64	أقوم بغلق تطبيقات الأمان ومكافحة الفيروسات على الهاتف أثناء استخدام التطبيق	العدد	29	41	90	82	58	3.33	1.21	متوسط (سالب)
		%	9.7	13.7	30	27.3	19.3			
65	أوافق على الوصول الى الصور ومقاطع الفيديو والتسجيلات الشخصية أثناء استخدام التطبيق	العدد	31	47	95	69	58	3.25	1.23	متوسط (سالب)
		%	10.3	15.7	31.7	23	19.3			
66	أوافق على فتح الكاميرا في أي وقت أثناء استخدام ا لتطبيق	العدد	33	44	78	90	55	3.30	1.23	متوسط (سالب)
		%	11	14.7	26	30	18.3			
67	أوافق على فتح الميكرفون أثناء استخدام التطبيق	العدد	39	30	87	76	68	3.35	1.29	متوسط (سالب)
		%	13	10	29	25.3	22.7			
68	أسمح للتطبيق بالاحتفاظ بالصور ومقاطع الفيديو التي قمت باعدادها أثناء استخدام التطبيق .	العدد	35	39	76	86	64	3.35	1.27	متوسط (سالب)
		%	11.7	13	25.3	28.7	21.3			
69	أوافق على ربط اعدادات التطبيق بحسابي على التطبيقات الاخرى مثل الفيس بوك facebook وخلافه	العدد	34	36	91	79	60	3.32	1.24	متوسط (سالب)
		%	11.3	12	30.3	26.3	20			
70	أوافق على السماح للتطبيق بالتعرف على بيانات شبكة ال wi-Fi المستخدمة	العدد	30	39	93	84	54	3.31	1.19	متوسط (سالب)
		%	10	13	31	28	18			

71	أوافق على السماح للتطبيق بالوصول الى بيانات جهات الاتصال لدي .	العدد	35	35	75	90	65	3.38	1.26	متوسط (سالب)
		%	11.7	11.7	25	30	21.7			
المتوسط المرجح والإنحراف المعياري للبعد السادس كلياً								3.33	0.935	

جدول (6) ملخص قيم المتوسط المرجح والوزن النسبي والمستوى لأبعاد سلوك الحماية البيومترية

م	الأبعاد	المتوسط المرجح	الانحراف المعياري	مستوى الشيوع
1	**الشدة المدركة**	2.97	0.501	متوسط
2	**القابلية للتأثير المدركة**	2.84	0.819	متوسط
3	**الكفاءة الذاتية**	2.76	0.861	متوسط
4	**فعالية الاستجابة**	2.81	0.875	متوسط
5	**المكافئات**	2.82	0.729	متوسط
6	**الاستراتيجيات المستخدمة**	3.33	0.935	متوسط

من النتائج الموضحة بالجدولين (5، 6) يتبين أن نسب المئوية لبدائل التقييم الخمسة على المفردات الإيجابية والسلبية وما اسفرت عنه نتائج قيم المتوسطات على جميع المفردات في كل من الأبعاد الستة لسلوك الحماية البيومترية (الشدة المدركة ، القابلية للتأثير المدركة ، الكفاءة الذاتية ، فعالية الإستجابة ، المكافئات ، الاستراتيجيات المستخدمة) أنها تتراوح بين ضعيفة أو مرتفع (سالب) إلى متوسطة ، وهذا يشير إلى أن انخفاض المظاهر السلوكية الدالة على سلوك دافع الحماية البيومترية لدى طلبة الجامعة مستخدمي تطبيقات التزييف العميق وأنه في أحسن الأحوال لا يتعد المستوى المتوسط لدى أفرد عينة الدراسة .

نتائج الدراسة:

السمات الديموغرافية لعينة الدراسة:

- **نسبة مستخدمي وغير مستخدمي تطبيقات التزييف العميق**

جدول رقم (7) عينة الدراسة من مستخدمي وغير مستخدمي تطبيقات التزييف العميق

البيان	العدد	النسبة المئوية
مستخدمي تطبيقات التزييف العميق	300	% 76.9
غير مستخدمي تطبيقات التزييف العميق	90	% 23.1
الإجمالي	390	% 100

تشير نتائج الجدول رقم (7) إلى إرتفاع نسبة مستخدمى تطبيقات التزييف العميق بنسبة 76,9% مقارنة بغير مستخدمي تطبيقات التزييف العميق بنسبة 23,1% وقد يفسر تلك النتيجة طبيعة تطبيقات التزييف العميق وسهولة استخدامها بالإضافة إلى ما أشارت له نتائج الدراسات والتي أشارت لسلاسة الإستخدام والتقاط صورة «سيلفي» ذاتية بسيطة للشخص ، يستطيع من خلالها تجسيد الشخصية الشهيرة التي يحلم بأن يتقمصها في دقائق معدودة وقد يفسر هذه النتيجه أيضا طبيعة عينة الدراسة من شباب الجامعات في المرحلة العمرية مرحلة الشباب وحب الإستطلاع وشغف تجربة كل ما هو جديد وانتشار تطبيقات التزييف العميق مجانية الإستخدام عبر وسائل التواصل الإجتماعي وتوفرها في متجر التطبيقات بالمجان، وتتفق تلك النتيجة مع دراسة **Jarvis (2021)** حول سهولة استخدام تطبيقات التزييف العميق لبعض الأغراض الترفيهية أو التجميلية ومنها توفير فلتر تجميلي متعدد الإستخدامات .

- **مستخدمي تطبيقات التزييف العميق وفقا للجنس**

جدول رقم (8) عينة الدراسة من مستخدمي تطبيقات التزييف العميق وفقا للجنس

البيان	العدد	النسبة المئوية
الذكور	173	% 57.7
الإناث	127	% 42.3
الإجمالي	300	% 100

تشير نتائج الجدول رقم (8) إلى إرتفاع نسبة الذكور لمستخدمى تطبيقات التزييف العميق 57.7% مقارنة بنسبة بالإناث 42.3% ، وقد يفسر هذه النتيجه ذلك طبيعة عينة الدراسة من حيث ان الذكور تستخدم كل ما هو جديد مثل تطبيقات التزييف العميق المجانية عبر وسائل التواصل

الإجتماعي وتوفرها في متجر التطبيقات بالمجان، واتفقت تلك النتيجة مع ما أشارت اليه نتائج دراسة بن صالح الناصري (2019) التي تم تطبيقها على عينة من طلبة التعليم ما بعد الأساسي؛ فكان الذكور من فئة الشباب هم الأكثر استخداما لتطبيقات التزيف العميق بالمقارنة بفئة الإناث؛ ويفسر تلك النتيجة بأن الأسر العمانية تعطي الثقة الكاملة للذكور أثناء استخدام وسائل التواصل الاجتماعيّ علي عكس الإناث، بالإضافة لتطرق الذكور عينة الدراسة لبعض المواقع المجانية –بطرق غير مشروعه ومخالفة للآداب العامة– على خلاف عينة الإناث التي اتسمت بالحياء في استخدام وسائل التواصل الاجتماعي.

- **بيان عينة الدراسة مستخدمي تطبيقات التزييف العميق وفقا لنوع الجامعة**

جدول رقم (9) عينة الدراسة من مستخدمي تطبيقات التزييف العميق وفقا لنوع الجامعة

البيان	العدد	النسبة المئوية
جامعات حكومية	154	% 51.3
جامعات خاصة	146	% 48.7
الإجمالي	300	% 100

تشير نتائج الجدول رقم (9) إلى إرتفاع نسبة مستخدمى تطبيقات التزييف العميق في الجامعات الحكومية بنسبة 51.3% مقارنة بالجامعات الخاصة بنسبة 48.7%، ويمكن تفسير إرتفاع نسبة مستخدمى تطبيقات التزييف العميق في الجامعات الحكومية مقارنة بالجامعات الخاصة هذه النتيجة في ضوء توجه الجامعات الحكومية للتحول للأنظمة الإلكترونية والمبادرات الرقمية وانتشار ثقافة التعليم عن بعد وتطبيقات التعرف على الوجه .

- **بيان عينة الدراسة مستخدمي تطبيقات التزييف العميق وفقا طبيعة الإقامة :**

جدول رقم (10) عينة الدراسة من مستخدمي تطبيقات التزييف العميق وفقا طبيعة الإقامة

البيان	العدد	النسبة المئوية
حضر	**210**	**% 70**
ريف	**90**	**% 30**
الإجمالي	**300**	**% 100**

تشير نتائج الجدول رقم (10) إلى إرتفاع نسبة مستخدمى تطبيقات التزييف العميق فى الحضر الى 70% مقارنة بالريف 30% أوضحت النتائج إرتفاع نسبة مستخدمى تطبيقات التزييف العميق

فى الحضر الى مقارنة بالريف وقد يفسر هذه النتيجة انتشار المعرفة والتكنولوجيا عبر الحدود للحضر خاصة في ظل انتشار فيروس كرونا وزيادة معدل استخدام الهواتف وفلاتر التصوير والعديد من المتطلبات التي قد تخالف طبيعة العادات والتقاليد والقيود المجتمعية المتحفظة إلى حد ما

- **بيان عينة الدراسة مستخدمي تطبيقات التزييف العميق وفقا لنظام الهاتف المستخدم :**

جدول رقم (11) عينة الدراسة من مستخدمي تطبيقات التزييف العميق وفقا لنظام الهاتف المستخدم

البيان	العدد	النسبة المئوية
Android	235	% 78.3
IOS	65	% 21.7
الإجمالي	300	% 100

تشير نتائج الجدول رقم (11) إلى إرتفاع نسبة مستخدمى تطبيقات التزييف العميق لمستخدمى هواتف Android الى 78.3% مقارنة بمستخدمى هواتف IOS 21.7% وقد يفسر هذه النتيجة نظام الحماية الخاص بهواتف ايفون مقارنة بنظام الحماية الذي توفره هواتف اندرويد، نظرا لما تسمح به اعدادات الإستخدام داخل هواتف اندرويد حيث تسمح للمستخدم بتحميل التطبيقات من مصادر خارجية وهذا ما يجعلها عرضة للإختراق أكثر من هواتف ابل.

- **معدلات استخدام تطبيقات التزييف العميق المختلفة (ن = 003) :**

جدول رقم (12) معدلات استخدام تطبيقات التزييف العميق المختلفة (ن = 300)

البيان	العدد	النسبة المئوية
Jiggy	57	13.5
Wombo	57	13.5
Deep fake lab	51	12.1
Deep Art	**51**	**12.1**
My Heritage	**50**	**11.9**
Face swap live	**49**	**11.6**
Zao	**45**	**10.7**
Reface	**37**	**8.8**
Snap shat	**15**	**3.6**

Remini	9	2.2
إجمالي استجابات الطلبة (ن = 300)	421	% 100

تشير نتائج الجدول رقم (12) إلى تفاوت نسب استخدام تطبيقات التزييف العميق من مستخدمى تطبيقات التزييف العميق من Jiggy و Wombo فكانت نسب كلاهما 13.5% لكل تطبيق وهى الأعلى نسبة فى التطبيقات بينما تطبيقى Deep fake lab وDeep Art كانت نسب كلاهما 12.1% لكل تطبيق مقارنة بتطبيق My Heritage الذى كانت نسبته 11.9% وكذلك تطبيق Face swap live 11.6% كما كان تطبيق Zao 10.7% بينما تطبيق Reface 8.8% ولكن جاءت نسبة تطبيق Snap shat 3.6% بينما Remini بنسبة 2.2% ، وقد يفسر هذه النتيجة ما توفره بعض التطبيقات الأكثر استخداما مقارنة بالتطبيقات الأخرى حيث تعددت استخدامتها مابين تقليد للمشاهيرومطابقة للصوت وتعبيرات الوجه ،إضافة إلى اشتياق البعض لرؤية احبائهم الذين فقدوهم ليجعلهم التطبيق يتحدثوا ويغنوا مرة أخرى وكل مايتطلبه صورة واحدة للشخص وذلك وفق لطبيعة عمل التطبيق عن طريق فرض بعض الخوارزميات، من خلال استخدام الذكاء الاصطناعي والتي تقوم بتصميم فيديو يحاكى حركات الابتسامة والعينين لصورة أى شخص، من اجل التوصل الى الفيديو النهائي،ويتفق هذامع ما أشارت له دراسة Kwok 2021 حول مخاطر الاستخدام الضار لمقاطع الفيديو المزيفة العميقة في عمليات الاحتيال والخداع وإساءة استخدام البيانات البيومتريَّة والتطورات السريعة في تقنية deepfake وتأثيرها المحتمل على انتحال الشخصيات.

- **معدلات القيام بعملية النسخ الاحتياطي BackUp للتطبيقات على الهاتف :**

جدول رقم (13) معدلات القيام بعملية النسخ الاحتياطي BackUp للتطبيقات على الهاتف

البيان	العدد	النسبة المئوية
يومياً	32	% 10.7
أسبوعياً	61	% 20.3
شهرياً	93	% 31
لا أستخدم النسخ الإحتياطي	87	% 29
لا أعلم ما هو النسخ الإحتياطي	27	% 9
الإجمالي	300	% 100

تشير نتائج الجدول رقم (13) إلى نسب القيام بعملية النسخ الاحتياطى BackUp للتطبيقات على الهاتف المتفاوته يوميا 10.7% واسبوعيا 20.3% بينما شهريا 31% مقارنة بمن لا يستخدموا النسخ الإحتياطي 29% بينما المستخدمين الذين لا يعلمون ما هو النسخ الإحتياطى 9% . وتشير هذه النتيجة إلى مخاطر استخدام كافة التطبيقات التي تعتمد على البيانات البيومترية والقياس الحيوية عبر الأجهزة الإلكترونية والهواتف الذكية دون عمل نسخ احتياطي بشكل دوري وخاطر ذلك على اختراق خصوصية الأفراد وهذا ما أشارت إليه دراسة **محمد سعد ابراهيم (2021)** حول التعرف على بنود الحق في الخصوصيَّة الرَّقميَّة وما يتعرض له مستخدمو تطبيقات الذَّكَاء الْإِصْطِنَاعِيّ وتقنيات التعلم العميق من اختراقات أمنية دون أن يشعر المستخدم، وتوصلت نتائج الدراسة إلى العلاقة بين استخدام التطبيقات التي تعتمد على تقنيات التعرف على الوجه والانتهاكات الشخصيَّة والاجتماعية والمهنيَّة والسياسيَّة والتجارية للخصوصيَّة الرَّقميَّة لمستخدميها، وأشارت الدراسة إلى ضرورة التدخل التشريعي والقانوني لتعزيز وحماية حق المستخدم في الأمان الرقمي

- **دوافع استخدام تطبيقات التزييف العميق DeepFake من وجهة نظر الطلبة**

جدول رقم (14) دوافع استخدام تطبيقات التزييف العميق DeepFake من وجهة نظر الطلبة

البيان	العدد	النسبة المئوية
الحصول على نسخة متحركة من الصورة مع الوجه والعينين والفم تتحرك.	85	% 13.5
تحريك الصور القديمة والحنين لأشخاص في الماضي وغادروا الحياة., التنمر والسخرية من الآخرين	75	% 11.9
أداة لتصميم مقاطع الفيديو .deepfake	67	% 10.6
خلق صورا عميقة تنتمي لعالم الفن والهياكل القديمة واللوحات	60	% 9.5
التقاط الصور بأبعاد 3D	53	% 8.4
الترفيه والتسلية وانتاج مقاطع كوميدية	41	% 6.5
التنمر والسخرية من الآخرين	40	% 6.3
مزامنة الشفاه إلى وجه غنائي	40	% 6.3
الفضول وشغف تجربة كل ماهو جديد	37	% 5.9
تركيب وجهك بصيغة gif	36	% 5.7
للتعلم والتدريب ومعرفة المزيد عن التقنية	27	% 4.3
الفراغ والوحدة	22	% 3.5
محاكاة الشخصيات السياسية ومحاكاة المشاهير بفيديوهات مزيفه	20	% 3.2

اختيار مقطع فيديو من مكتبة المسلسلات الدرامية والأفلام وإعادة تمثيله	14	% 2.2
انتاج ونشر مقاطع غير لائقة مخالفة للآداب العامة	13	% 2.1
إجمالي استجابات الطلبة (ن = 300)	**630**	**%** 001

تشير نتائج الجدول رقم (14) إلى تفاوت نسب الدوافع لاستخدام تطبيقات التزييف العميق DeepFake من وجهة نظر الطلبة التى انحصرت بين اعلى نسبة كانت 13.5 % وهى الحصول على نسخة متحركة من الصورة مع الوجه والعينين والفم تتحرك واقل نسبة 2.1 % انتاج ونشر مقاطع غير لائقة مخالفة للآداب العامة وتتفق هذه النتيجة مع ما أشارت له نتائج الدراسات السابقة وما أوضحته حول دوافع استخدام الشباب لتطبيقات التَّزْيِيف الْعَمِيق وتمثلت في: استخدام التطبيقات بغرض الترفيه والمحاكاة الساخرة، والأغراض الإجرامية، والابتزاز.

- **أسباب إنتشار تطبيقات التزييف العميق من وجهة نظر الطلبة :**

جدول رقم (15) أسباب إنتشار تطبيقات التزييف العميق من وجهة نظر الطلبة

البيان	العدد	النسبة المئوية
مجانية التطبيقات وسهولة استخدامها من قبل الجميع	91	16
سهولة استخدام هذه البرامج والتطبيقات لغير المتخصصين	87	15.3
التوجه العام لعمليات التجميل و هوس الفلاتروالسيلفي لتحسين الصورة	78	13.7
استخدامه في صناعة السينما كأنتاج فيلم حديث لممثل شهير رحل أو محاكاة الوقائع التاريخية للعلماء والمفكرين الراحلين	72	12.7
الرغبة في الهروب من الواقع ومشاعر الحزن	67	11.8
التسلية والترفيه ومشاركة الأصدقاء والأقارب ومشاركة الآخرين بفيديوهات مضحكة	47	8.3
لقصف والتشهير بالمشاهير والقادة والسياسين ولأغراض اجرامية	45	7.9
محاكاة حركة الفم البشري أثناء الكلام أو الغناء بدقة عالية	41	7.2
الحصول على إعجابات كثيرة من الأصدقاء عبر وسائل التواصل في عالم افتراضي وليس حقيقيا	40	7.1
إجمالي استجابات الطلبة (ن = 300)	**568**	**100%**

تشير نتائج الجدول رقم (15) إلى أسباب إنتشار تطبيقات التزييف العميق من وجهة نظر الطلبة حيث ان اعلى نسبة كانت مجانية التطبيقات وسهولة استخدامها من قبل الجميع 16 % واقل نسبة

الحصول على إعجابات كثيرة من الأصدقاء عبر وسائل التواصل في عالم افتراضي وليس حقيقيا 7.1 % ، وفي هذا الشأن نجد أن دراسة(2020)Acquisti & Loewenstein أشارت إلى أن الأشخاص الذين يهتمون بخصوصياتهم ويتخذون خطوات لحمايتها، يستطيعون إدارة الخصوصيَّة بفعالية عبر الإنترنت، وأرجعت السبب الرئيس لعدم تمكن المستهلكين من الحصول على المستويات المرغوبة من الخصوصيَّة هو عدم فهمهم لكيفية جمع بياناتهم ونشرها واستخدامها، ويتفق مع هذا الاتجاه ما أشارت إليه دراسة(2020) Furini & Prandi حول سلوكيات المستخدمين الرَّقميَّة للتطبيقات دون دراية بمعايير الحماية الرَّقميَّة لبياناتهم البيومتريَّة؛ حيث يقوم المستخدمون بتثبيت التطبيقات الترفيهية في أغلب الأوقات دون قراءة شروط وأحكام الاستخدام؛ والنتيجة هي أن خصوصياتهم في خطر متزايد.

نتائج التحقق من فروض الدراسة:

أولاً: نتائج التحقق من الفرض الأول:

ينص الفرض الأول على أنه: **(توجد فروق دالة إحصائياً في سلوك الحماية البيومتريَّة بين الطلبة مستخدمي تطبيقات التَّزْييف الْعَمِيق والطلبة غير مستخدمي تطبيقات التَّزْييف الْعَمِيق).** وللتحقق من هذا الفرض استخدمت الباحثة اختبارات لدلالة الفروق بين متوسط عينتين مستقلتين، وبحساب دلالة الفروق بين مجموعة الطلبة الذين يستخدمون تطبيقات التَّزْييف الْعَمِيق والطلبة التي لا يستخدمون تطبيقات التَّزْييف الْعَمِيق في كل من الأبعاد الفرعية الستة (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت، الإستراتيجيات المستخدمة) والدرجة الكلية على مقياس سلوك الحماية البيومترية، وأظهرت المعالجة الإحصائية باستخدام برنامج الحزم الإحصائية SPSS إصدار (26) النتائج الموضحة بالجدول (16).

جدول (16) نتائج اختبارات دلالة الفروق بين مستخدمي تطبيقات التَّزْييف الْعَمِيق وغير مستخدمي تطبيقات التَّزْييف الْعَمِيق على مقياس سلوك الحماية البيومتريَّة (ن = 390)

النمط	المجموعات	العدد	المتوسط	الانحراف المعياري	درجات الحرية	قيمة ت	الدلالة
الشدة المدركة	مستخدمو تطبيقات التزييف العميق	300	46.12	7.03	388	6.46 -	0.01
	غير مستخدمي تطبيقات التزييف ا لعميق	90	52.81	9.02			

النمط	المجموعات	العدد	المتوسط	الانحراف المعياري	درجات الحرية	قيمة ت	الدلالة
القابلية للتأثير المدركة	مستخدمو تطبيقات التزييف العميق	300	38.67	10.53	388	3.34 -	0.01
	غير مستخدمي تطبيقات التزييف العميق	90	43.84	13.50			
الكفاءة الذاتية	مستخدمو تطبيقات التزييف العميق	300	34.63	10.44	388	3.73 -	0.01
	غير مستخدمي تطبيقات التزييف العميق	90	40.24	12.53			
فعالية الاستجابة	مستخدمو تطبيقات التزييف العميق	300	29.60	9.01	388	4.67 -	0.01
	غير مستخدمي تطبيقات التزييف العميق	90	35.57	10.26			
المكافآت	مستخدمو تطبيقات التزييف العميق	300	21.91	5.50	388	4.00 -	0.01
	غير مستخدمي تطبيقات التزييف العميق	90	25.04	6.30			
الاستراتيجيات المستخدمة	مستخدمو تطبيقات التزييف العميق	300	30.33	7.75	388	1.284	غير دالة إحصائياً
	غير مستخدمي تطبيقات التزييف العميق	90	28.85	10.34			
الدرجة الكلية	مستخدمو تطبيقات التزييف العميق	300	201.29	31.88	388	5.54 -	0.01
	غير مستخدمي تطبيقات التزييف العميق	90	226.37	36.47			

يتبين من نتائج الجدول (16) قبول الفرض الأول؛ حيث يتبين وجود فروق دالة إحصائياً

بين الطلبة مستخدمي تطبيقات التَّزْييف الْعَمِيق وغير مستخدمي تطبيقات التَّزْييف الْعَمِيق في الأبعاد الفرعية الخمسة (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت) والدرجة الكلية لسلوك الحماية البيومترية؛ حيث بلغت قيم ت (6.46، 3.34، 3.73، 4.67، 4، 5.54) على الترتيب، وجميعها قيم دالة إحصائيا عند مستوى دلالة (0.01)، وبناء على قيم المتوسطات لدرجات الأبعاد الفرعية والدرجة الكلية لكل من مجموعة المستخدمين وغير المستخدمين لتطبيقات التَّزْييف الْعَمِيق يتبين أن اتجاه الفروق جاء جميعه لصالح مجموعة الطلبة غير مستخدمي تطبيقات التزييف العميق. وهذه النتائج تعني أن الطلبة غير مستخدمي تطبيقات التَّزْييف الْعَمِيق كانوا أعلى في معظم الأبعاد الفرعية (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت) والدرجة الكلية لسلوك الحماية البيومتريَّة مقارنة بالطلبة مستخدمي تطبيقات التزييف العميق، بينما لا توجد فروق بين المستخدمين وغير المستخدمين لتطبيقات التَّزْييف الْعَمِيق في الإستراتيجيات المستخدمة لحماية الخصوصيَّة البيومترية.

ثانياً: نتائج التحقق من الفرض الثاني:

ينص الفرض الثاني على أنه (**توجد فروق دالة إحصائياً بين الذكور والإناث مستخدمي تطبيقات التَّزْييف الْعَمِيق في سلوك الحماية البيومتريَّة**). وللتحقق من هذا الفرض استخدمت الباحثة اختبارات لدلالة الفروق بين متوسط عينتين مستقلتين، وبحساب دلالة الفروق بين الذكور والإناث في كل من الأبعاد الفرعية الستة (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت، الإستراتيجيات المستخدمة) والدرجة الكلية على مقياس سلوك الحماية البيومترية، أظهرت المعالجة الإحصائية باستخدام برنامج الحزم الإحصائية SPSS إصدار (26) النتائج الموضحة بالجدول (17).

جدول (17) نتائج اختبارات لدلالة الفروق بين مجموعتي الذكور والإناث مستخدمي تطبيقات التزييف العميق على الأبعاد الفرعية والدرجة الكلية لمقياس سلوك الحماية البيومتريَّة (ن = 300)

النمط	المجموعات	العدد	المتوسط	الانحراف المعياري	درجات الحرية	قيمة ت	الدلالة
الشدة المدركة	ذكور	173	46.77	7.60	298	2.261-	0.05
	إناث	127	48.88	8.45			
القابلية للتأثير المدركة	ذكور	173	38.67	10.52	298	2.097-	0.05
	إناث	127	41.47	12.51			
الكفاءة الذاتية	ذكور	173	34.76	10.19	298	2.103-	0.05
	إناث	127	37.50	12.29			

النمط	المجموعات	العدد	المتوسط	الانحراف المعياري	درجات الحرية	قيمة ت	الدلالة
فعالية الاستجابة	ذكور	173	29.49	8.47	298	3.157-	0.01
	إناث	127	33.00	10.73			
المكافآت	ذكور	173	21.89	5.12	298	2.590-	0.01
	إناث	127	23.64	6.57			
الاستراتيجيات المستخدمة	ذكور	173	31.62	7.50	298	4.003	0.01
	إناث	127	27.77	9.09			
الدرجة الكلية	ذكور	173	203.23	31.51	298	2.253 -	0.05
	إناث	127	212.28	37.88			

يتبين من نتائج الجدول (17) قبول الفرض الثاني؛ حيث يتبين وجود فروق دالة إحصائياً بين الذكور والإناث في جميع الأبعاد الفرعية الستة (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت، الإستراتيجيات المستخدمة) والدرجة الكلية لسلوك الحماية البيومترية؛ حيث بلغت قيم ت (2.261، 2.097، 2.103، 3.157، 2.590، 4.003، 2.253) على الترتيب، وجميعها قيم دالة إحصائيا عند مستوى دلالة (0.01) بالنسبة للأبعاد: فعالة الاستجابة، و المكافآت، والاستراتيجيات المستخدمة، ودالة عند مستوى دلالة (0.05) بالنسبة للأبعاد: الشدة المدركة، والقابلية للتأثير المدركة، والكفاءة الذاتية والدرجة الكلية لسلوك الحماية البيومترية، كما يتبين قيم المتوسطات لكل من الذكور والإناث أن اتجاه الفروق جاءت جميعها لصالح الإناث فيما عدا بعد الإستراتيجيات المستخدمة جاء لصالح مجموعة الذكور، بمعنى أن الإناث كُنَّ مرتفعات في كل من: أبعاد الشدة المدركة، والقابلية للتأثير المدركة، والكفاءة الذاتية، وفعالية الاستجابة، و المكافآت، وكذلك الدرجة الكلية لسلوك الحماية البيومتريَّة مقارنة بالذكور؛ في حين أن الذكور كانوا أعلى في الإستراتيجيات المستخدمة لتحقيق سلوك الحماية البيومتريَّة مقارنة بالإناث.

ثالثاً: نتائج التحقق من الفرض الثالث:

ينص الفرض الثالث على أنه: **توجد فروق دالة إحصائياً بين المقيمين في الريف والمقيمين في الحضر من مستخدمي تطبيقات التَّزْييف الْعَمِيق في سلوك الحماية البيومترية.** وللتحقق من هذا الفرض استخدمت الباحثة اختبارات لدلالة الفروق بين متوسط عينتين مستقلتين، وبحساب دلالة الفروق بين المقيمين في الحضر والمقيمين في الريف في كل من الأبعاد الفرعية الستة (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت، الإستراتيجيات

المستخدمة) والدرجة الكلية على مقياس سلوك الحماية البيومترية، أظهرت المعالجة الإحصائية باستخدام برنامج الحزم الإحصائية SPSS إصدار (26) النتائج الموضحة بالجدول (18).

جدول (18) نتائج اختبارات لدلالة الفروق بين مجموعتي المقيمين في الحضر والمقيمين في الريف من مستخدمي تطبيقات التَّزْييف الْعَمِيق على الأبعاد الفرعية والدرجة الكلية لمقياس سلوك الحماية البيومتريَّة (ن = 300).

النمط	المجموعات	العدد	المتوسط	الانحراف المعياري	درجات الحرية	قيمة ت	الدلالة
الشدة المدركة	المقيمون في الحضر	210	47.87	8.29	298	0.674	غير دال إحصائياً
	المقيمون في الريف	90	47.18	7.40			
القابلية للتأثير المدركة	المقيمون في الحضر	210	40.40	12.45	298	1.268	غير دال إحصائياً
	المقيمون في الريف	90	38.57	8.70			
الكفاءة الذاتية	المقيمون في الحضر	210	36.77	12.46	298	2.007	0.05
	المقيمون في الريف	90	33.95	7.09			
فعالية الاستجابة	المقيمون في الحضر	210	31.95	10.57	298	2.711	0.01
	المقيمون في الريف	90	28.70	6.44			
المكافآت	المقيمون في الحضر	210	23.17	6.41	298	2.444	0.01
	المقيمون في الريف	90	21.38	3.95			
الاستراتيجيات المستخدمة	المقيمون في الحضر	210	29.43	9.19	298	1.776-	غير دال إحصائياً
	المقيمون في الريف	90	31.31	6.11			

النمط	المجموعات	العدد	المتوسط	الانحراف المعياري	درجات الحرية	قيمة ت	الدلالة
الدرجة الكلية	المقيمون في الحضر	210	209.61	37.60	298	1.958	0.05
	المقيمون في الريف	90	201.12	25.44			

يتبين من نتائج الجدول (18) قبول الفرض الثالث جزئياً؛ حيث يتبين وجود فروق دالة إحصائيا بين الطلبة المقيمين في الحضر والطلبة المقيمين في الريف في بعض الأبعاد الفرعية (الكفاءة الذاتية، فعالية الاستجابة، المكافآت) والدرجة الكلية لسلوك الحماية البيومترية؛ حيث بلغت قيم ت (2.007، 2.711، 2.444، 1.958) على الترتيب، حيث جاءت دلالة الفروق على متغيري: فعالية الاستجابة/ والمكافآت في سلوك الحماية البيومتريَّة عند مستوى دلالة (0.01)، بينما جاءت دلالة الفروق على متغير الكفاءة الذاتية والدرجة الكلية لسلوك الحماية البيومتريَّة دالة عند مستوى دلالة (0.05)، ويلاحظ أن اتجاه الفروق في الأبعاد الأربعة لسلوك الحماية البيومتريَّة جاء لصالح مجموعة الطلبة المقيمين في الحضر؛ بمعنى أن الطلبة المقيمين في الحضر كانوا مرتفعين مقارنة بالطلبة المقيمين في الريف في كل من: الكفاءة الذاتية، وفعالية الاستجابة، و المكافآت، وكذلك الدرجة الكلية على مقياس سلوك الحماية البيومترية، بينما يتبين أنه لا توجد فروق دالة إحصائياً بين الطلبة المقيمين في الحضر والطلبة المقيمين في الريف في الأبعاد الفرعية الثلاثة (الشدة المدركة، القابلية للتأثير المدركة، الإستراتيجيات المستخدمة) لسلوك الحماية البيومترية، حيث بلغت قيم ت (0.674، 1.268، 1.776) على الترتيب، وجميعها قيم غير دالة إحصائياً.

رابعاً: نتائج التحقق من الفرض الرابع:

ينص الفرض الرابع على أنه: **توجد فروق دالة إحصائياً بين طلبة الجامعات الحكومية وطلبة الجامعة الخاصة مستخدمي تطبيقات التَّزْييف الْعَمِيق في سلوك الحماية البيومترية.** وللتحقق من هذا الفرض استخدمت الباحثة اختبارات لدلالة الفروق بين متوسط عينتين مستقلتين، وبحساب دلالة الفروق بين طلبة الجامعات الحكومية وطلبة الجامعات الخاصة في كل من الأبعاد الفرعية الستة (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت، الإستراتيجيات المستخدمة) والدرجة الكلية على مقياس سلوك الحماية البيومترية، أظهرت المعالجة الإحصائية باستخدام برنامج الحزم الإحصائية SPSS إصدار (26) النتائج الموضحة بالجدول (19).

جدول (19) نتائج اختبارات لدلالة الفروق بين طلبة الجامعات الحكومية وطلبة الجامعات الخاصة مستخدمي تطبيقات التَّزْييف الْعَمِيق على الأبعاد الفرعية والدرجة الكلية لمقياس سلوك الحماية البيومتريَّة (ن = 300)

النمط	المجموعات	العدد	المتوسط	الانحراف المعياري	درجات الحرية	قيمة ت	الدلالة
الشدة المدركة	طلبة الجامعات الحكومية	154	48.92	8.96	298	2.827	0.01
	طلبة الجامعات الخاصة	146	46.33	6.69			
القابلية للتأثير المدركة	طلبة الجامعات الحكومية	154	41.06	12.35	298	1.876	غير دالة إحصائياً
	طلبة الجامعات الخاصة	146	38.58	10.36			
الكفاءة الذاتية	طلبة الجامعات الحكومية	154	36.27	11.77	298	0.560	غير دالة إحصائياً
	طلبة الجامعات الخاصة	146	35.55	10.56			
فعالية الاستجابة	طلبة الجامعات الحكومية	154	31.97	9.97	298	1.842	غير دالة إحصائياً
	طلبة الجامعات الخاصة	146	29.93	9.18			
المكافآت	طلبة الجامعات الحكومية	154	23.46	5.72	298	2.556	0.01
	طلبة الجامعات الخاصة	146	21.76	5.84			
الاستراتيجيات المستخدمة	طلبة الجامعات الحكومية	154	30.15	8.95	298	0.336	غير دالة إحصائياً
	طلبة الجامعات الخاصة	146	29.82	7.85			
الدرجة الكلية	طلبة الجامعات الحكومية	154	211.87	36.52	298	2.492	0.05
	طلبة الجامعات الخاصة	146	202.00	31.76			

يتبين من نتائج الجدول (19) قبول الفرض الرابع جزئياً؛ حيث يتبين وجود فروق دالة إحصائيا بين طلبة الجامعات الحكومية وطلبة الجامعات الخاصة في بعدي (الشدة المدركة، المكافآت)

والدرجة الكلية على مقياس سلوك الحماية البيومترية؛ حيث بلغت قيم ت (2.827، 2.556، 2.492) على الترتيب، وجاءت دلالة الفروق على متغيري الشدة المدركة والمكافآت في سلوك الحماية البيومتريَّة عند مستوى دلالة (0.01)، بينما جاءت الدرجة الكلية لسلوك الحماية البيومتريَّة دالة عند مستوى دلالة (0.05)، ويلاحَظ أن اتجاه الفروق في البعدين (الشدة المدركة، المكافآت) وكذلك الدرجة الكلية لسلوك الحماية البيومتريَّة جاء لصالح مجموعة طلبة الجامعات الحكومية؛ بمعنى أن طلبة الجامعات الحكومية كانوا مرتفعين مقارنة بطلبة الجامعات الخاصة في كل من: الشدة المدركة، و المكافآت والدرجة الكلية على مقياس سلوك الحماية البيومترية. بينما يتبين أنه لا توجد فروق دالة إحصائياً بين طلبة الجامعات الحكومية وطلبة الجامعات الخاصة في الأبعاد الفرعية الأربعة (القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، الإستراتيجيات المستخدمة) لسلوك الحماية البيومترية، حيث بلغت قيم ت (1.876، 0.560، 1.842، 0.336) على الترتيب، وجميعها قيم غير دالة إحصائياً.

خامساً: نتائج التحقق من الفرض الخامس:

ينص الفرض الخامس على أنه: **توجد فروق دالة إحصائياً بين الطلبة مستخدمي هاتف من بنظام Android والطلبة مستخدمي هاتف بنظام IOS ومستخدمي تطبيقات التَّزْييف الْعَمِيق في سلوك الحماية البيومترية.** وللتحقق من هذا الفرض استخدمت الباحثة اختبارات لدلالة الفروق بين متوسط عينتين مستقلتين، وبحساب دلالة الفروق بين الطلبة مستخدمة الهاتف من طراز Android والطلبة مستخدمي الهاتف من طراز IOS في كل من الأبعاد الفرعية الستة (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت، الإستراتيجيات المستخدمة) والدرجة الكلية على مقياس سلوك الحماية البيومترية، أظهرت نتائج المعالجة الإحصائية باستخدام برنامج الحزم الإحصائية SPSS إصدار (26) عن النتائج الموضحة بالجدول (20).

جدول (20) نتائج اختبارات لدلالة الفروق بين مستخدمي هاتف من بنظام Android والطلبة مستخدمي هاتف بنظام IOSومستخدمي تطبيقات التَّزْييف الْعَمِيق على الأبعاد الفرعية والدرجة الكلية لمقياس سلوك الحماية البيومتريَّة (ن = 300).

النمط	المجموعات	العدد	المتوسط	الانحراف المعياري	درجات الحرية	قيمة ت	الدلالة
الشدة المدركة	مستخدمو هاتف Android	235	47.03	7.70	298	2.601-	0.01
	مستخدمو هاتف IOS	65	49.93	8.80			
القابلية للتأثير المدركة	مستخدمو هاتف Android	235	39.00	10.67	298	2.490-	0.01
	مستخدمو هاتف IOS	65	42.96	13.62			
الكفاءة الذاتية	مستخدمو هاتف Android	235	34.81	10.06	298	3.332-	0.01
	مستخدمو هاتف IOS	65	39.95	13.93			
فعالية الاستجابة	مستخدمو هاتف Android	235	30.08	8.68	298	3.118 -	0.01
	مستخدمو هاتف IOS	65	34.23	12.01			
المكافآت	مستخدمو هاتف Android	235	21.87	5.26	298	4.420 -	0.01
	مستخدمو هاتف IOS	65	25.38	6.93			
الاستراتيجيات المستخدمة	مستخدمو هاتف Android	235	31.10	7.53	298	4.456	0.01
	مستخدمو هاتف IOS	65	26.00	10.15			
الدرجة الكلية	مستخدمو هاتف Android	235	203.91	31.71	298	3.046-	0.01
	مستخدمو هاتف IOS	65	218.47	41.74			

يتبين من نتائج الجدول (20) قبول الفرض الخامس؛ حيث يتبين وجود فروق دالة إحصائيا بين الطلبة مستخدمي الهاتف بنظام Android والطلبة مستخدمي الهاتف بنظام IOS في جميع الأبعاد الفرعية الستة (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت، الإستراتيجيات المستخدمة) وكذلك الدرجة الكلية لسلوك الحماية البيومترية؛ حيث بلغت

قيم ت (2.601، 2.490، 3.332، 3.118، 4.420، 4.456، 3.046) على الترتيب، وجميعها قيم دالة عند مستوى دلالة (0.01)، كما يلاحظ من قيم المتوسطات لمجموعتي الطلبة مستخدمي الهاتف بنظام Android ومجموعة الطلبة مستخدمي الهاتف بنظام IOS على الأبعاد الفرعية والدرجة الكلية لسلوك الحماية البيومتريَّة يشير إلى أن اتجاه الفروق في الأبعاد الفرعية الخمسة (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت) والدرجة الكلية لسلوك الحماية البيومتريَّة جاء لصالح مجموعة الطلبة مستخدمي الهاتف بنظام IOS؛ فيما عدا بُعد (الإستراتيجيات المستخدمة) فقد جاء اتجاه الفروق لصالح مجموعة الطلبة مستخدمي الهاتف بنظام Android، وهذه النتائج تعني أن الطلبة مستخدمي الهاتف بنظام IOS كانوا أعلى مقارنة بالطلبة مستخدمي الهاتف بنظام Android في كل من: الشدة المدركة، والقابلية للتأثير المدركة، والكفاءة الذاتية، وفعالية الاستجابة، و المكافآت وكذلك الدرجة الكلية لسلوك الحماية البيومترية، في حين أن الطلبة مستخدمي الهاتف بنظام Android كانوا أعلى من الطلبة مستخدمي الهاتف بنظام IOS في الإستراتيجيات المستخدمة لتحقيق سلوك الحماية البيومترية.

سادساً: نتائج التحقق من الفرض السادس:

ينص الفرض السادس على أنه: **تختلف درجة سلوك الحماية البيومتريَّة لدى مستخدمي تطبيقات التَّزْييف الْعَمِيق باختلاف الجنس (ذكور، إناث)، طبيعة الإقامة (حضر، ريف)، نوع الجامعة (حكومية، خاصة)، والتفاعل بينهم.** وللتحقق من هذا الفرض قامت الباحثة بإجراءين: الأول: تم حساب المتوسطات والانحرافات المعيارية لدرجة سلوك الحماية البيومتريَّة لدى مجموعات الدراسة المختلفة من حيث متغيرات النوع (ذكور، إناث) ومحل الإقامة (حضر، ريف) ونوع الجامعة (حكومية، خاصة). الثاني: تم استخدام أسلوب تحليل التباين الثلاثي 3- way ANOVA لتحليل الفروق بين مجموعات الدراسة في درجة سلوك الحماية البيومتريَّة وفقا لمتغيرات النوع ومحل الإقامة ونوع الجامعة وبحث تأثير التفاعلات بينهم على سلوك الحماية البيومتريَّة لدى أفراد عينة الدراسة، وقد أسفرت نتائج المعالجة الإحصائية باستخدام برنامج الحزم الإحصائية للعلوم الاجتماعيَّة SPSS (إصدار 26) عن النتائج الموضحة بجدولين (21،22):

جدول (21) المتوسطات الحسابية والانحرافات المعيارية في سلوك الحماية البيومتريَّة لدى مجموعات الدراسة مستخدمي تطبيقات التَّزْييف الْعَمِيق وفقا لمتغيرات الجنس وطبيعة الإقامة ونوع الجامعة (ن = 300)

المتغيرات المستقلة			المتوسط	الانحراف المعياري	العدد
الجنس	طبيعة الإقامة	نوع الجامعة			

المتغيرات المستقلة			المتوسط	الانحراف المعياري	العدد
ذكور	حضر	حكومية	208.15	34.04	69
		خاصة	197.23	30.13	59
		الكلي	203.12	32.64	128
	ريف	حكومية	204.54	31.93	31
		خاصة	201.35	19.29	14
		الكلي	203.55	28.41	45
	الكلي	حكومية	207.04	33.28	100
		خاصة	198.02	28.31	73
		الكلي	203.23	31.51	173
إناث	حضر	حكومية	227.81	43.03	38
		خاصة	212.77	41.29	44
		الكلي	219.74	42.52	82
	ريف	حكومية	204.18	29.40	16
		خاصة	195.65	16.73	29
		الكلي	198.68	22.13	45
	الكلي	حكومية	220.81	40.69	54
		خاصة	205.97	34.61	73
		الكلي	212.28	37.88	127

المتغيرات المستقلة			المتوسط	الانحراف المعياري	العدد
الكلي	حضر	حكومية	215.14	38.46	107
		خاصة	203.87	35.98	103
		الكلي	209.61	37.60	210
	ريف	حكومية	204.42	30.77	47
		خاصة	197.51	17.58	43
		الكلي	201.12	25.44	90
	الكلي	حكومية	211.87	36.52	154
		خاصة	202.00	31.76	146
		الكلي	207.06	34.58	300

جدول (22) نتائج تحليل التباين الثلاثي 3- way ANOVA لأثر متغيرات الجنس وطبيعة الإقامة ونوع الجامعة والتفاعل بينهم على سلوك الحماية البيومتريَّة لدى مستخدمي تطبيقات التزييف العميق.

مصدر التباين	مجموع المربعات	درجات الحرية	متوسطات المربعات	قيمة ف	الدلالة الإحصائية
التباين الأساسي (النموذج)	28137.42	7	4019.63	3.56	0.01
الجنس (ذكور، إناث)	3017.90	1	3017.90	2.67	غير دال إحصائياً
طبيعة الإقامة	5758.46	1	5758.46	5.102	0.05
نوع الجامعة	5052.18	1	5052.18	4.476	0.05
الجنس x طبيعة الإقامة	6053.42	1	6053.42	5.363	0.05
الجنس x نوع الجامعة	318.43	1	318.43	0.282	غير دال إحصائياً
طبيعة الإقامة x نوع الجامعة	721.39	1	721.39	0.639	غير دال إحصائياً
الجنس x طبيعة الاقامة x نوع الجامعة	5.29	1	5.295	0.005	غير دال إحصائياً
الخطأ Error	329589.24	292	1128.73	-	-

المجموع الكلي	13220708	300	-	-	-
المجموع الكلي المعدل	357726.66	299	-	-	-

تشير نتائج تحليل التباين الثلاثي 3- way ANOVA الموضحة في الجدول (22) إلى قبول الفرض السادس؛ حيث جاءت قيمة التباين الأساس لنموذج تحليل التباين دالة إحصائياً عند مستوى دلالة (0.01)، ويمكن توضيح نتائج التحليل تفصيلا على النحو الآتي:

(1)يوجد تأثير دال إحصائياً لمتغير طبيعة الإقامة (حضر، ريف) في تباين درجات أفراد عينة الدراسة على الدرجة الكلية لمقياس سلوك الحماية البيومترية؛ حيث يتبين من نتائج الجدول (7) أن قيمة ف لدلالة الفروق بين مجموعة الطلبة المقيمين في الحضر ومجموعة الطلبة المقيمين في ريف في سلوك الحماية البيومتريَّة قد بلغت (5.102) وهي قيمة دالة إحصائياً عند مستوى دلالة (0.05)، ويتبين من قيم المتوسطات لكلا المجموعتين أن اتجاه الفروق لصالح مجموعة الطلبة المقيمين في الحضر.

(2)يوجد تأثير دال إحصائياً لمتغير نوع الجامعة (حكومية، خاصة) في تباين درجات أفراد عينة الدراسة على الدرجة الكلية لمقياس سلوك الحماية البيومترية؛ حيث يتبين من نتائج الجدول (22) أن قيمة ف لدلالة الفروق بين مجموعة الطلبة في الجامعات الحكومية ومجموعة الطلبة في الجامعات الخاصة في سلوك الحماية البيومتريَّة قد بلغت (4.476) وهي قيمة دالة إحصائياً عند مستوى دلالة (0.05)، ويتبين من قيم المتوسطات لكلا المجموعتين أن اتجاه الفروق لصالح مجموعة طلبة الجامعات الحكومية.

(3)يوجد تأثير دال إحصائياً لتفاعل متغيري (الجنس، طبيعة الإقامة) في تباين درجات أفراد عينة الدراسة على الدرجة الكلية لمقياس سلوك الحماية البيومترية؛ حيث يتبين من نتائج الجدول (22) أن قيمة ف لدلالة الفروق بين مجموعات الدراسة تبعا لتفاعل متغيري (الجنس، طبيعة الإقامة) في سلوك الحماية البيومتريَّة قد بلغت (5.363) وهي قيمة دالة إحصائياً عند مستوى دلالة (0.05)، ويتبين من قيم المتوسطات لمجموعات الدراسة الأربعة (ذكور حضر = 203.12، ذكور ريف = 203.55، إناث حضر = 219.74، إناث ريف = 198.68) أن اتجاه الفروق لصالح مجموعة الطالبات الإناث المقيمات في الحضر.

(4)لا يوجد تأثير دال إحصائياً لمتغير النوع (ذكور، إناث) في تباين درجات أفراد عينة الدراسة على الدرجة الكلية لمقياس سلوك الحماية البيومترية؛ حيث يتبين من نتائج الجدول (22) أن قيمة ف للفروق بين مجموعتي الذكور والاناث في سلوك الحماية البيومتريَّة قد بلغت (2.67) وهي قيمة غير دالة إحصائياً، بما يشير إلى عدم وجود فروق دالة إحصائياً بين الذكور والإناث من طلبة المرحلة الجامعية في درجة سلوك الحماية البيومتريَّة لديهم.

(5)لا يوجد تأثير دال إحصائياً لتفاعل متغيري (الجنس، نوع الجامعة) في تباين درجات أفراد عينة الدراسة على الدرجة الكلية لمقياس سلوك الحماية البيومترية؛ حيث يتبين من نتائج الجدول (22)

أن قيمة ف لدلالة الفروق بين مجموعات الدراسة تبعا لتفاعل متغيري (الجنس، نوع الجامعة) في سلوك الحماية البيومتريَّة قد بلغت (0.282) وهي قيمة غير دالة إحصائياً.

(6)لا يوجد تأثير دال إحصائياً لتفاعل متغيري (طبيعة الإقامة، نوع الجامعة) في تباين درجات أفراد عينة الدراسة على الدرجة الكلية لمقياس سلوك الحماية البيومترية؛ حيث يتبين من نتائج الجدول (22) أن قيمة ف لدلالة الفروق بين مجموعات الدراسة تبعا لتفاعل متغيري (طبيعة الإقامة، نوع الجامعة) في سلوك الحماية البيومتريَّة قد بلغت (0.639) وهي قيمة غير دالة إحصائياً.

(7)لا يوجد تأثير دال إحصائياً لتفاعل المتغيرات الثلاثة (الجنس، طبيعة الإقامة، نوع الجامعة) في تباين درجات أفراد عينة الدراسة على الدرجة الكلية لمقياس سلوك الحماية البيومترية؛ حيث يتبين من نتائج الجدول (22) أن قيمة ف لدلالة الفروق بين مجموعات الدراسة تبعا لتفاعل المتغيرات الثلاثة (الجنس، طبيعة الإقامة، نوع الجامعة) في سلوك الحماية البيومتريَّة قد بلغت (0.005) وهي قيمة غير دالة إحصائياً.

سابعاً: نتائج التحقق من الفرض السابع:

ينص الفرض السابع على أنه: **لا توجد فروق دالة إحصائياً بين الطلبة متقني اللغة الانجليزية وغير متقنيها في سلوك الحماية البيومترية.** وللتحقق من هذا الفرض استخدمت الباحثة اختبارات لدلالة الفروق بين متوسط عينتين مستقلتين، وبحساب دلالة الفروق بين مجموعة الطلبة الذين يجيدون اللغة الأجنبية والطلبة الذين لا يجيدون اللغة الأجنبية في كل من الأبعاد الفرعية الستة (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت، الإستراتيجيات المستخدمة) والدرجة الكلية على مقياس سلوك الحماية البيومترية، وأظهرت المعالجة الإحصائية باستخدام برنامج الحزم الإحصائية SPSS إصدار (26) النتائج الموضحة بالجدول (23).

جدول (23) نتائج اختبارات لدلالة الفروق بين الطلبة متقني اللغة الإنجليزية، والطلبة غير متقنيها من مستخدمي تطبيقات التَّزْبِيف الْعَمِيق على الأبعاد الفرعية والدرجة الكلية لمقياس سلوك الحماية البيومتريَّة (ن = 300)

النمط	المجموعات	العدد	المتوسط	الانحراف المعياري	درجات الحرية	قيمة ت	الدلالة
الشدة المدركة	متقنو اللغة الانجليزية	249	47.72	8.26	298	0.015-	غير دالة إحصائياً
	غير متقني اللغة الانجليزية	51	47.74	6.95			

النمط	المجموعات	العدد	المتوسط	الانحراف المعياري	درجات الحرية	قيمة ت	الدلالة
القابلية للتأثير المدركة	متقنو اللغة الانجليزية	249	39.96	11.54	298	0.094	غير دالة إحصائياً
	غير متقني اللغة الانجليزية	51	39.80	11.28			
الكفاءة الذاتية	متقنو اللغة الانجليزية	249	36.42	11.58	298	1.468	غير دالة إحصائياً
	غير متقني اللغة الانجليزية	51	33.88	9.03			
فعالية الاستجابة	متقنو اللغة الانجليزية	249	31.17	10.03	298	0.411	غير دالة إحصائياً
	غير متقني اللغة الانجليزية	51	30.56	7.30			
المكافآت	متقنو اللغة الانجليزية	249	22.83	6.09	298	0.927	غير دالة إحصائياً
	غير متقني اللغة الانجليزية	51	22.00	4.29			
الاستراتيجيات المستخدمة	متقنو اللغة الانجليزية	249	29.63	8.70	298	1.440-	غير دالة إحصائياً
	غير متقني اللغة الانجليزية	51	31.52	6.95			
الدرجة الكلية	متقنو اللغة الانجليزية	249	207.76	35.65	298	0.422	غير دالة إحصائياً
	غير متقني اللغة الانجليزية	51	205.50	28.84			

يتبين من نتائج الجدول (23) قبول الفرض السابع؛ حيث يتبين عدم وجود فروق دالة إحصائياً بين الطلبة متقني اللغة الانجليزية والطلبة غير متقني اللغة الانجليزية في جميع الأبعاد الفرعية الستة (الشدة المدركة، القابلية للتأثير المدركة، الكفاءة الذاتية، فعالية الاستجابة، المكافآت، الإستراتيجيات المستخدمة) والدرجة الكلية لسلوك الحماية البيومترية؛ حيث بلغت قيم ت (0.015، 0.094، 1.46، 0.411، 0.927، 1.44، 0.422) على الترتيب، وجميعها قيم غير دالة إحصائيا، وهذا يعني أنه لا توجد فروق دالة إحصائياً في الأبعاد الفرعية والدرجة الكلية في سلوك الحماية

البيومتريَّة ترجع إلى إتقان أو عدم إتقان الطلبة للغة الإنجليزية، أو بمعني آخر: إن سلوك الحماية البيومتريَّة لا يرجع إلى مدى إتقان الطالب للغة الإنجليزية من عدمه.

مناقشة النتائج:

- إرتفاع نسبة مستخدمى تطبيقات التزييف العميق مقارنة بغير مستخدمي تطبيقات التزييف العميق.

ويمكن تفسير هذه النتيجه في ضوء طبيعة عينة الدراسة من شباب الجامعات في المرحلة العمرية (مرحلة الشباب) وحب الإستطلاع وشغف تجربة كل ما هو جديد وانتشار هوس تجربة التطبيقات التي توفر فلاتر ومحسنات للصور بين الشباب وهذا ماتوفره هذه التطبيقات ، بالإضافة لتوفرها في متجر التطبيقات بالمجان وتتفق تلك النتيجه مع ما رصدته شركة Sensity للتكنولوجيا حول ارتفاع عدد مقاطع الفيديو المفبركة على الإنترنت –على مدى الأشهر الستة الأولى من العام الحالي 2021، حيث تضاعف عددها ليبلغ 49081ألف مقطع فيديو مزيف.

- إرتفاع نسبة الذكور لمستخدمى تطبيقات التزييف العميق مقارنة بنسبة بالإناث وتتفق هذه النتيجة مع ما توصلت له نتائج دراسة بن صالح الناصري (2019) التي تم تطبيقها على عينة من طلبة التعليم ما بعد الأساسي؛ فكان الذكور من فئة الشباب هم الأكثر إستخداما للتطبيقات الإلكترونية والأكثر عرضة لانتهاك حقوقهم الرَّقميَّة بالمقارنة بفئة الإناث؛ وتفسر نتائج دراسة بن صالح تلك النتيجة بأن الأسر العمانية تعطي الثقة الكاملة للذكور أثناء استخدام وسائل التواصل الاجتماعيّ علي عكس الإناث، بالإضافة لتطرق الذكور عينة الدراسة لبعض المواقع المجانية –بطرق غير مشروعه والمخالفة للآداب العامة– على خلاف عينة الإناث التي اتسمت بالحياء في استخدام وسائل التواصل الاجتماعي، بالإضافة لغياب نشر ثقافة الحقوق الرَّقميَّة في الدول العربية مما يؤثر إيجابا على زيادة الانتهاكات الرَّقميَّة لمستخدمي وسائل التواصل الاجتماعي.

إرتفاع نسبة مستخدمى تطبيقات التزييف العميق في الجامعات الحكومية مقارنة بالجامعات الخاصة ويمكن تفسير هذه النتيجة في ضوء توجه الجامعات الحكومية للتحول للأنظمة الإلكترونية وانتشار ثقافة التعليم عن بعد ، كما أوضحت النتائج إرتفاع نسبة مستخدمى تطبيقات التزييف العميق فى الحضر الى مقارنة بالريف.

- أوضحت نتائج الدراسة تطبيقات التزييف العميق الأكثر إستخداما من قبل عينة الدراسة وتمثلت التطبيقات الأكثر استخداما في تطبيقى Jiggy و Wombo يليهما تطبيقي Deepfakelab وDeep Art.
- إرتفاع نسبة مستخدمى تطبيقات التزييف العميق لمستخدمى هواتف Android مقارنة بمستخدمى هواتف IOS نظرا لإختلاف أنظمة الحماية الخاص بهواتف ايفون مقارنة بنظام الحماية الذي توفره هواتف اندرويد، وكذلك ما تسمح به اعدادات الإستخدام داخل هواتف اندرويد حيث تسمح للمستخدم بتحميل التطبيقات من مصادر خارجية وهذا ما يجعلها عرضة للإختراق أكثر من هواتف ابل.

توصيات الدراسة:

- ضرورة تطوير مصنفات وتطبيقات التعلم العميق، التي يمكنها توظيف الذكاء الاصطناعي لفحص الميزات الأولية لمقاطع الفيديو للإشارة إلى مدى أصالتها عبر العلامات المائية للفيديو البيومتري، وكذلك تدريب برامج تعلم آلي لتخطي وتجنب الإختراقات الأمنية الرقمية.
- إصدار رخص إلكترونية دولية للمبرمجين لمزاولة البرمجة وإنشاء البرمجيات المختلفة بحيث يصبح كل برنامج أو خوارزمية ذو هوية معروفة المصدر والمنشأ حول العالم، ونقر بصعوبة هذا الإجراء إلا أنه سيلعب دوراً بارزاً في تحجيم استخدام التقنية السلبية للتزييف العميق والحد من انتشارها تقنياً.
- ضرورة التوعية بين الشباب بأهمية البيانات الرقمية البيومترية وسبل اختراقها عبر التطبيقات الذكاء الإصطناعي المختلفة وأهمية دافع سلوك حماية الخصوصية.

هوامش:

أولاً: باللغة العربية

آيات قاسي، حورية. (2021). تطبيقات تعقّب مخالطي المصابين ب (كوفيد19) بين ضرورة حماية الصحة العامة ومخاطر انتهاك الخصوصية-39 ,(1)16, **revue critique de droit et sciences politiques** . 61.

بن ناصرالناصري، خلفان. (2019). مدى تأثير شبكات التواصل الاجتماعي في الحقوق الرقمية لدى طلبة التعليم ما بعد الأساسي (11-12) بمدارس سلطنة عمان. **المجلة التربوية لكلية التربية بسوهاج**، 67(67)، 436-450.

ليطوش، دليلة. (2019). الحماية القانونية للحق في الخصوصية الرقمية للمستهلك الإلكتروني. **مجلة العلوم الإنسانية**، 171-179.

سعد إبراهيم، محمد. (2021). الحق فى الخصوصية الرقمية فى إطار ثورة البيانات وأنماط التدخلات التشريعية والدولية. **مجلة البحوث والدراسات الإعلامية**،15(15)، 1-40.

العثمني،محمد. (2021). تقنية التعرُّف إلى الوجه ومكافحة الجريمة في المطارات العربية. **أوراق السياسات الأمنية**، 2(1)،1-10.

القرني،سعد. (2021). العلاقة بين نمط التفكير ونشر الخصوصية عبر الإعلام الاجتماعي الجديد. **مجلة البحوث الإعلامية**، 59(2)، 551-600.

المعداوي،محمد.(2018).حمايةالخصوصيةالمعلوماتية للمستخدم عبر شبكات مواقع التواصل الاجتماعي-دراسة مقارنة. **مجلة كلية الشريعة والقانون بطنطا**: مجلة فصلية علمية محكمة،33(4)، 1926-2057.

ثانياً: باللغة الانجليزية

Acquisti, A., Brandimarte, L., & Loewenstein, G. (2020). Secrets and likes: the drive for privacy and the difficulty of achieving it in the digital age. **Journal of Consumer Psychology**, **30**(4), 736-758

Agarwal, S., Farid, H., El-Gaaly, T., & Lim, S. N. (2020, December). Detecting deep-fake videos from appearance and behavior. In 2020 IEEE International Workshop **on Information Forensics and Security (WIFS)** (pp. 1-6).

Ahmed, S. R. A., & Sonuç, E. (2021). Deepfake detection using rationale-augmented convolutional neural network. **Applied Nanoscience**, 1-9.

Berghoff, C., Neu, M., & von Twickel, A. (2021). The Interplay of AI and Biometrics: Challenges and Opportunities. **Computer, 54**(09), 80-85.

Bode, L. (2021). Deepfaking Keanu: YouTube deepfakes, platform visual effects, and the complexity of reception. **Convergence, 27**(4), 919-934.

Chen, H., Beaudoin, C. E., & Hong, T. (2017). Securing online privacy: An empirical test on Internet Scam victimization, online privacy concerns, and privacy protection behaviors. **Computers in Human Behavior**, 70, 291-302.

Chen, M., Liao, X., & Wu, M. (2021). PulseEdit: Editing Physiological Signal in Facial Videos for Privacy Protection.

Chowdhury, S. A. K., & Lubna, J. I. (2020, July). Review on Deep Fake: A looming Technological Threat. In **2020 11th International Conference on Computing, Communication and Networking Technologies (ICCCNT)** (pp. 1-7).

Chuang, Y. H., Lei, C. L., & Shiu Jr, H. (2021). How to Design a Secure Anonymous Authentication and Key Agreement Protocol for Multi-Server Environments and Prove Its Security. **Symmetry, 13**(9), 1629.

Cozma, R., & Muturi, N. (2021). It's Not All Doom and Gloom:: Protection Motivation Theory Factors That Reverse the Negative Impact of Social Media Use on Compliance and Protective Health Behaviors. **Southwestern Mass Communication Journal, 37**(1).

Dargan, S., & Kumar, M. (2020). A comprehensive survey on the biometric recognition systems based on physiological and behavioral modalities. **Expert Systems with Applications, 143**, 113-114.

Delgado-Santos, P., Stragapede, G., Tolosana, R., Guest, R., Deravi, F., & Vera-Rodriguez, R. (2021). A Survey of Privacy Vulnerabilities of Mobile Device Sensors. **arXiv preprint arXiv**:2106.10154.

Fletcher, J. (2018). Deepfakes, Artificial Intelligence, and Some Kind of Dystopia: The New Faces of Online Post-Fact Performance. **Theatre Journal,** 70(4): 455–471. Project MUSE, doi:10.1353/tj.2018.0097

Furini, M., Mirri, S., Montangero, M., & Prandi, C. (2020). Privacy Perception when Using Smartphone Applications. **Mob Networks Appl.**, 25(3), 1055-1061.

Grindley, E. J., Zizzi, S. J., and Nasypany, A. M. (2008). Use of protectiomotivation theory, affect, and barriers to understand and predict adherence to outpatient rehabilitation. Physical Therapy. **Journal of American Physical Theraphy Association**, 88(12):1529–1540.

Haag, S., Siponen, M., & Liu, F. (2021). Protection motivation theory in information systems security research: A review of the past and a road map for the future. **ACM SIGMIS Database: the DATABASE for Advances in Information Systems, 52**(2), 25-67.

Hasan, H. R., & Salah, K. (2019). Combating Deepfake Videos Using Blockchain and Smart Contracts. **IEEE Access**, 7: 41596–41606.

Jarvis, L. (2021). Deepfake-ification: A Postdigital Aesthetics of Wrongness in Deepfakes and Theatrical Shallowfakes. Avatars, Activism and Postdigital Performance: **Precarious Intermedial Identities**, 89.

Johnston, B. A. C. and Warkentin, M. (2010). Fear Appeals and Information security Behaviors: An Empirical Study. **Ministry of Education Official Website**, 34(3):549–566.

Kim, A. Y., & Kim, T. S. (2016). Factors Influencing the Intention to Adopt Identity Theft Protection Services: severity vs Vulnerability. **In PACIS** (p. 68).

Kokolakis, S. (2017). Privacy attitudes and privacy behavior: A review of current research on the privacy paradox phenomenon. **Computers & Security**, **64**, 122-134.

Komkova, G., Amelin, R., & Kulikova, S. (2020, May). Legal protection of personal image in digital relations: leading trends. In **6th International Conference on Social, economic, and academic leadership** (ICSEAL-6-2019) (pp. 382-390). Atlantis Press.

Kwok, A. O., & Koh, S. G. (2021). Deepfake: a social construction of technology perspective. **Current Issues in Tourism, 24**(13), 1798-1802.

Laishram, L., Rahman, M. M., & Jung, S. K. (2021, February). Challenges and Applications

of Face Deepfake. **In International Workshop on Frontiers of Computer Vision** (pp. 131-156). Springer, Cham.

LEE, J. Y., & Al Khaldi, N. (2020). Exploring the ethical implications of new media technologies: A survey of online platform users' digital literacy and its effects on digital trust and privacy awareness. 1-2. Abstract from **70th Annual International Communication Association Conference (ICA 2020),** Washington D.C, United States.

Li, Q., Dong, P., & Zheng, J. (2020). Enhancing the security of pattern unlock with surface EMG-based biometrics. **Applied Sciences**, **10**(2), 541.

Mahdavifar, S., & Ghorbani, A. A. (2019). Application of deep learning to cybersecurity: A survey. **Neurocomputing,** 347, 149-176.

Marett, K., McNab, A. L., & Harris, R. B. (2011). Social networking websites and posting personal information: An evaluation of protection motivation theory. **AIS Transactions on Human-Computer Interaction, 3**(3), 170-188.

Martin, K. D., Borah, A., & Palmatier, R. W. (2017). Data privacy: Effects on customer and firm performance. **Journal of Marketing, 81**(1), 36-58.

MCMC (2014). Communications & Multimedia Pocket Book of Statistic.

Nemec Zlatolas, L., Welzer, T., Heri˘cko, M., and H¨olbl, M. (2015). Privacy antecedents for SNS self- disclosure: The case of Facebook. **Computers in Human Behavior**, 45:158–167.

Newland, M. C. (2019). An information theoretic approach to model selection: A tutorial with Monte Carlo confirmation. **Perspectives on behavior science,** 42(3), 583-616.

Palladino, B. E., Menesini, E., Nocentini, A., Luik, P., Naruskov, K., Ucanok, Z., & Scheithauer, H. (2017). Perceived Severity of Cyberbullying: Differences and Similarities across Four Countries. **Frontiers in Psychology,** 8, 1524.

Salleh, N., Hussein, R., Mohamed, N., Abdul, N. S., Ahlan, A. R., and Aditiawarman, U. (2012). Examining Information Disclosure Behavior on Social Network Sites Using Protection Motivation Theory, Trust and Risk. **Journal of Internet Social Networking & Virtual Communities**, 2012.

Sayler, K. M., & Harris, L. A. (2020). **Deep fakes and national security. Congressional Research SVC Washington United States.**

Schneider, S., Fürsich, F. T., & Werner, W. (2011). Biometric methods for species recognition in Trigonia Bruguière (Bivalvia; Trigoniidae): a case study from the Upper Jurassic of Western Europe. **Paläontologische Zeitschrift,** 85(3), 257-267.

Sedek, M., Mahmud, R., Jalil, H. A., & Daud, S. M. (2012). Types and levels of ubiquitous technology use among ICT undergraduates. **Procedia-Social and Behavioral Sciences,** 64, 255-264.

Sedik, A., Hammad, M., Abd El-Latif, A. A., El-Banby, G. M., Khalaf, A. A., Abd El-Samie, F. E., & Iliyasu, A. M. (2021). Deep Learning Modalities for Biometric Alteration Detection in 5G Networks-Based Secure Smart Cities. **IEEE Access**, 9, 94780-94788.

Stern, T., & Kumar, N. (2017). Examining privacy settings on online social networks: a protection motivation perspective. **International Journal of Electronic Business,**

13(2-3), 244-272.

Tesfagergish, S. G., Damaševičius, R., & Kapočiūtė-Dzikienė, J. (2021, September). Deep Fake Recognition in Tweets Using Text Augmentation, Word Embeddings and Deep Learning. In International Conference on Computational Science and Its Applications (pp. 523-538).

Trifiletti, E., Shamloo, S. E., Faccini, M., & Zaka, A. (2022). Psychological predictors of protective behaviours during the Covid-19 pandemic: Theory of planned behaviour and risk perception. **Journal of community & applied social psychology, 32**(3), 382-397 .

Visvikis, D., Le Rest, C. C., Jaouen, V., & Hatt, M. (2019). Artificial intelligence, machine (deep) learning and radio (geno) mics: definitions and nuclear medicine imaging applications. **European journal of nuclear medicine and molecular imaging,** 46(13), 2630-2637.

Vithessonthi, C. (2010). Knowledge sharing, social networks and organizational transformation. The Business Review, **Cambridge, 15**(2):99-10

Wojewidka, J. (2020). The deepfake threat to face biometrics. **Biometric Technology Today**, (2), 5-7.

Yang, W. C., & Tsai, J. C. (2020). Deepfake Detection Based on No-Reference Image Quality Assessment (NR-IQA). **Forensic Science Journal, 19**(1), 29-38.

Yao, X., Zhang, L., Du, J., & Gao, L. (2021). Effect of Information-Motivation-Behavioral model based on protection motivation theory on the psychological resilience and quality of life of patients with type 2 DM. **Psychiatric Quarterly, 92**(1), 49-62.

Yavuzkiliç, S., Akhtar, Z., Sengür, A., & Siddique, K. (2021). DeepFake Face Video Detection Using Hybrid Deep Residual Networks and LSTM Architecture. In **AI and Deep Learning in Biometric Security** (pp. 81-104).

Yu, P., Xia, Z., Fei, J., & Lu, Y. (2021). A Survey on Deepfake Video Detection. **IET Biometrics**.