وزارة التعليم العالي والبحث العلمي

جامعة بابل

كلية التربية للعلوم الصرفة

قسم الفيزياء

مراجعة منهجية لتقنيات الكشف عن تزوير الهوية في أنظمة التعرف على الوجه المعتمدة على التعلم العميق

مشروع مقدم إلى مجلس كلية التربية للعلوم الصرفة/جامعة بابل
وهو جزء من متطلبات نيل درجة بكالوريوس في الفيزياء

من قبل

نور إحسان علي

بإشراف

د. إنتهاء عبدالله الجبوري

1447هـ 2026م

بسم الله الرحمن الرحيم

﴿وَأَنْ لَيْسَ لِلْإِنْسَانِ إِلَّا مَا سَعَىٰ ﴿٣٩﴾
وَأَنَّ سَعْيَهُ سَوْفَ يُرَىٰ ﴿٤٠﴾ ثُمَّ يُجْزَاهُ
الْجَزَاءَ الْأَوْفَى ﴿٤١﴾﴾

صدق الله العلي العظيم

سورة النجم

الإهداء

إلهي لا يطيب الليل إلا بشكرك ولا يطيب النهار إلا بطاعتك ولا تطيب اللحظات إلا بذكرك ولا تطيب الآخرة إلا بعفوك ولا تطيب الجنة إلا برؤيتك يارب....

الى الذين من بركتهم استقام دربي ومن صمودهم استلهمت القوة سادتي وموالي ال محمد ﴿عليهم السلام﴾ ..... إلى مقام صاحب العصر والزمان الغائب الإمام المهدي ﴿عجل الله تعالى فرجه الشريف﴾.

إلى من كانت كل امنياتي... معلقة ببابه الى راية الوفاء ... الى القمر الذي اضاء لي الطريق ...الى سيدي ومولاي أبا الفضل العباس ﴿عليه السلام﴾ ...اهدي جهدي هذا علَه يكون قطرة في نهر وفاءه وسلاماً على من فدى ولم يؤذ ورحمة الله وبركاته.

إلى من كلله الله بالهيبة والوقار ... إلى من علمني العطاء بدون انتظار ... إلى من أحمل أسمه بكل افتخار..... (أرجو من الله ان يطيل في عمره) والدي العزيز حفظه الله.

إلى ملاكي في الحياة... إلى معنى الحب وإلى معنى الحنان والتفاني... إلى بسمة الحياة وسر الوجود إلى ... من كان دعائها سر نجاحي وحنانها بلسم جراحي .... إلى أغلى الحبايب (أمي الحبيبة).

إلى من قال فيه (سنشد عضدك باخيك) ... إلى ضلعي الثابت وأمان أيامي ... إلى من كان لي ينبوع ارتوي منه لخيرة ايامي وصفوها ... إلى من كانت أنفاسه تكفيني ونظراته ترويني (أخي الحبيب).

عظم المراد فهان الطريق فجاءت لذة الوصول لتزول مشقة السنين الحمد لله ما تناهى درب ولا ختم جهد ولا تم سعي إلا بفضله وكرمه الحمد لله الذي بفضله اختار لي الطريق وبفضله رضيت وبفضله اجتزت وأنهيت.

﴿وآخر دَعواهم أن الحمدُ للهِ رَبِّ العالمينَ﴾

الشكر والتقدير

بسم الله الرحمن الرحيم الحمد لله رب والصلاة والسلام على اشرف الأنبياء والمرسلين....

تتقدم الباحثة بخالص الشكر والتقدير إلى قسم الفيزياء والى جميع الأساتذة في كلية التربية للعلوم الصرفة – جامعة بابل لدعمهم المتواصل إلى طلبة الكلية في سبيل الارتقاء بالمستوى العلمي نحو الأفضل. كما لا يسع الباحثة وقد أنهت كتابة بحثها إلا أن تتقدم بخالص الشكر وعظيم الامتنان إلى الدكتورة إنتهاء عبدالله الجبوري على ما قدمته من رعاية علمية وتوجيهات قيمة وأراء سديدة كانت خيراً وعوناً لي في انجاز مهمتي فضلاً عن صبرها الجميل معي بكل ما الم بي من ظروف، طوال مدة اعداد هذا البحث خيراً وصبرها وسخائها، وفقها الله وسدد خطاها.

المستخلص

يتناول هذا البحث المقدم بعنوان (مراجعة منهجية لاحدث تقنيات الكشف عن تزوير الهوية (spoofing attacks) في أنظمة التعرف على الوجه المعتمدة على التعلم العميق) مراجعة لعدد من البحوث العلمية المنشورة في موضوعاً هاماً وبارزاً في المجالات التقنية المتنوعة الا وهي تقنيات الكشف عن تزوير الهوية المعتمدة على التعلم العميق.

توضح المراجعة كيفية قدرة الشبكات العصبية العميقة على التمييز بين الوجه الحقيقي والمزيف من خلال تحليل الخصائص البصرية والحركية والملمسية للوجه، كما يستعرض البحث ابرز الأساليب والخوارزميات الحديثة المستخدمة في هذا المجال مثل الشبكات التلافيفية (CNNs) والشبكات التوليدية الخصومية إضافة الى قواعد البيانات التي تستخدم لتدريب هذه النماذج، كما يسلط الضوء على التحديات القائمة ومنها صعوبة تعميم النماذج على أماكن مختلفة وضرورة تطوير أنظمة خفيفة وفعالة يمكن تطبيقها في الأجهزة المحمولة. ختاماً تؤكد هذه المراجعة على أهمية دمج تقنيات الذكاء الاصطناعي المتقدمة لتطوير أنظمة اكثر اماناً وموثوقية في مجال التحقق البيومتري .

قائمة المحتويات

الفصل الثالث

الفصل الرابع

الفصل الخامس

قائمة الاشكال

الفصل الأول

مقدمة عن التحقق البيومتري والتعرف على الوجه

1.1 المقدمة Introduction

في ظل الثورة التكنولوجية التي يشهدها العالم في العقود الأخيرة، أصبح هنالك تطوراً هائلاً في مجال التكنولوجيا الرقمية مما أفرز حاجة متزايدة إلى وسائل تحقق أكثر أماناً ودقة في التعرف على هوية الأفراد [1]. وقد أدى ذلك إلى بروز أنظمة التحقق البيومتري كأحد أهم الابتكارات في مجال أمن المعلومات والأنظمة الذكية [2]، يقوم هذا النوع من التحقق على استخدام الخصائص الحيوية أو السلوكية الفريدة لكل شخص مثل بصمة الإصبع، قزحية العين، نبرة الصوت أو ملامح الوجه، وذلك بهدف التحقق من الهوية بطريقة يصعب تزويرها أو انتحالها [3].

تُعَدّ تقنية التعرف على الوجه (Face Recognition) من أكثر تقنيات التحقق البيومتري شيوعاً وانتشاراً في الوقت الراهن لما تمتاز به من سهولة الاستخدام وعدم تطلبها لتلامس مباشر مع الجهاز، على عكس بعض الوسائل البيومترية الأخرى [4]. تعتمد هذه التقنية على معالجة الصور الرقمية وتحليل الملامح الهندسية للوجه مثل المسافات النسبية بين العينين، شكل الأنف، محيط الشفتين، حدود الفك والفم، ثم تحويل هذه الخصائص إلى تمثيل رقمي يُقارن بقاعدة بيانات لتحديد أو تأكيد هوية الشخص [5]. وقد وجدت تقنيات التعرف على الوجه تطبيقات واسعة في مجالات عديدة منها أنظمة المراقبة الأمنية في المطارات والمؤسسات الحكومية والهواتف الذكية والتحقق من الهوية في المصارف والجامعات وحتى في شبكات التواصل الاجتماعي [4]، كما أسهم التطور في الذكاء الاصطناعي وخوارزميات التعلم العميق في رفع دقة هذه الأنظمة وتقليل الأخطاء الناتجة عن اختلاف الإضاءة أو زوايا التصوير أو تعابير الوجه [2]. وتكمن أهمية أنظمة التعرف على الوجه في كونها وسيلة تحقق آمنة وسريعة وغير تلامسية، مما يجعلها مناسبة للتطبيقات التي تتطلب دقة عالية وسهولة استخدام، مثل المراقبة الذكية وأنظمة الحضور والانصراف والدفع الإلكتروني [4]. كما أن هذه التقنية تسهم في تعزيز الأمن العام وتبسيط عمليات التحقق في

المجالات الحساسة، فضلاً عن قابليتها للتكامل مع أنظمة الذكاء الاصطناعي لتطوير بيئات رقمية أكثر أماناً وكفاءة [2].

2.1 بيان المشكلة Problem Statement

تعد أنظمة التعرف على الوجه من أهم تقنيات التحقق البيومتري المستخدمة في مختلف التطبيقات الأمنية مثل الوصول إلى الأجهزة المصارف والمراقبة. مع ذلك تواجه هذه الأنظمة تحديًا كبيرًا يتمثل في هجمات تزوير الهوية Spoofing Attacks التي تحاول خداع النظام باستخدام صور أو فيديوهات أو أقنعة ثلاثية الأبعاد للوجه. تقلل هذه الهجمات من فعالية أنظمة التحقق البيومتري وقد تؤدي إلى انتهاك الخصوصية وسرقة الهوية.

رغم التقدم الكبير في نماذج التعلم العميق Deep Learning إلا أن العديد من التحديات ما زالت قائمة. من هذه التحديات تنوع هجمات التزوير حيث تختلف طرق التزوير بين الطباعة على الورق الفيديوهات المعاد تشغيلها أو الأقنعة ثلاثية الأبعاد مما يجعل اكتشافها صعبًا باستخدام نموذج واحد. تتأثر النماذج بالبيئة حيث تغيّر الإضاءة حركة الوجه بوجود الضوضاء أو جودة الكاميرا قد يقلل من دقة كشف التزوير. كذلك فأن نقص البيانات المتنوعة حيث يحتاج تدريب نماذج التعلم العميق إلى مجموعات من البيانات كبيرة ومتنوعة لكل نوع من أنواع التزوير وهذا غير متوفر دائمًا خاصة للهجمات الواقعية المعقدة، والكفاءة الحسابية حيث تتطلب النماذج العميقة موارد حاسوبية ضخمة ما يحد من إمكانية تطبيقها على الأجهزة منخفضة القدرة أو الوقت الحقيقي، وقلة المعايير الموحدة للتقييم حيث اختلاف طرق تقييم أداء النماذج بين الدراسات يصعب المقارنة بين التقنيات المختلفة.

3.1 أهداف البحث Research objectives

1. استعراض منهجي لتقنيات الكشف عن تزوير الهوية (Spoofing Attacks) في أنظمة التعرف على الوجه المعتمدة على التعلم العميق، مع توضيح الأساليب المستخدمة وتطورها عبر السنوات.
2. تصنيف الأساليب والتقنيات المختلفة حسب نوع التزوير (مثل الصور المطبوعة، الفيديوهات المعاد تشغيلها، الأقنعة ثلاثية الأبعاد) وبيئات الاختبار المستخدمة.
3. تقييم فعالية الأساليب المختلفة من حيث الدقة، الكفاءة الحسابية، والقدرة على التعامل مع التحديات الواقعية مثل تغيّر الإضاءة أو حركة الوجه.
4. تحديد نقاط القوة والضعف في كل تقنية، مع إبراز الفجوات البحثية التي تحتاج إلى تطوير وتحسين.
5. اقتراح توصيات مستقبلية لتطوير أنظمة كشف أكثر موثوقية ومرونة، بما يتيح استخدامها في التطبيقات الواقعية والأجهزة منخفضة الموارد.

هذه الأهداف تسهم في تعزيز فهم تقنيات الكشف عن تزوير الهوية (Spoofing Attacks) في أنظمة التعرف على الوجه المعتمدة على التعلم العميق لدعم التطبيقات العملية.

4.1 البحوث السابقة Literature Review

تناولت البحوث السابقة في مجال الكشف عن تزوير الهوية (Spoofing Attacks) في أنظمة التعرف على الوجه المعتمدة على التعلم العميق عدة تقنيات وأساليب متعددة [16]، في البداية اعتمدت الدراسات على السمات اليدوية (Handcrafted Features) والخوارزميات التقليدية مثل تحليل النصوع والملمس (Texture Analysis) وآليات التعرف الكلاسيكية، والتي كانت مناسبة للكشف عن حالات التزوير البسيطة [17].

مع تطور التعلم العميق (Deep Learning) ظهرت نماذج أكثر قدرة على التعامل مع التزوير المعقد [18]، بما في ذلك الشبكات العصبية التلافيفية (CNNs) والشبكات التوليدية

الخصومة (GANs)، التي حسّنت من دقة الكشف على الصور والفيديوهات المشوهة أو المعدلة. كما تم تطبيق نماذج متقدمة مثل SRCNN وSRGAN لتطوير أنظمة أكثر مرونة في التعامل مع الصور الواقعية وتحسين أداء الكشف [19].

ومن أبرز الأمثلة على الدراسات السابقة، Hassan T. Mohammad and others (2021) في دراستهم "Face Spoofing Detection Using Deep CNN" [20]، استخدموا شبكة CNN متخصصة لكشف هجمات القناع الثلاثي الأبعاد (3D Mask Attacks)، وحققوا دقة بلغت 99.88% مما يؤكد فعالية الشبكات العميقة في حالات التزوير المعقدة.

Kot, A. and others (2024) في بحثهم " Learning Deep Forest for Face Anti-Spoofing: An Alternative to the Neural Network Against Adversarial Attacks"، اقترحوا نموذج Deep Forest كبديل للشبكات العصبية، بهدف تقليل استهلاك الموارد الحسابية مع الحفاظ على الدقة العالية في كشف التزوير العدائي [21].

ركزت الأبحاث الحديثة بشكل خاص على تحديات البيانات الواقعية، مثل تغيّر الإضاءة، حركة الوجه، وجود الضوضاء أو انخفاض جودة الصورة، واستخدمت مجموعات بيانات متنوعة تشمل الصور الصناعية، صور كاميرات المراقبة، والبيانات البيومترية الطبية لتدريب النماذج [18]. ورغم التقدم، لا تزال هناك تحديات في الكفاءة الحسابية واحتياجات الموارد الضخمة للنماذج، مما دفع الباحثين لاستخدام تقنيات التعلم الانتقالي (Transfer Learning) لتحسين الدقة وتقليل حجم البيانات المطلوبة [19].

تعكس هذه الدراسات استمرار تركيز المجال على تطوير أساليب فعّالة وموثوقة للكشف عن تزوير الهوية في أنظمة التعرف على الوجه، مع مراعاة التحديات العملية والتقنية للبيئات الواقعية [17].

الفصل الثاني

أساليب الكشف غير المعتمدة على التعلم العميق ومجموعات البيانات

1.2 المقدمة Introduction

تُعدّ الأساليب التقليدية في توصيف المواد من الركائز الأساسية في علم فيزياء المواد، إذ أسهمت بشكل واضح في فهم العلاقة بين البنية المجهرية والخواص الفيزيائية لمختلف المواد [22]. وقد استُخدمت هذه الأساليب على نطاق واسع بسبب وضوح مبادئها الفيزيائية وسهولة تطبيقها مقارنة بالتقنيات المتقدمة [23]. كما تُعد نتائج هذه الأساليب مرجعاً أساسياً يُعتمد عليه لمقارنة وتفسير نتائج التقنيات الحديثة في دراسات توصيف المواد [24]. علاوة على ذلك، يركز تحليل الخصائص المجهرية على دراسة البنية الدقيقة للمواد، بما يشمل حجم الحبيبات وتوزيع الأطوار والعيوب البلورية وتأثيرها المباشر على الخواص الفيزيائية والميكانيكية [25]. وتُعد تقنيات المجهر الإلكتروني الماسح من أكثر الأساليب التقليدية استخداماً في فحص البنية المجهرية وتحليل التباينات البنيوية داخل المواد [24]. في حين يُستخدم المجهر الإلكتروني النافذ على نطاق واسع لدراسة التراكيب البلورية والعيوب الداخلية بدقة عالية [26].

من جهة أخرى، تكتسب تقنيات العمق التقليدية أهمية كبيرة في توصيف التدرج البنيوي والتركيبي داخل المواد، ولاسيما في الأغشية الرقيقة والمواد متعددة الطبقات [29]. وتهدف هذه التقنيات إلى دراسة التغيرات في التركيب الكيميائي والبنية البلورية مع العمق باستخدام أساليب تحليلية معتمدة تقليدياً [31]. كما تُستخدم تقنيات التحليل الطيفي والحيود بالأشعة السينية للحصول على معلومات غير إتلافية حول توزيع العناصر والبنية الداخلية للمادة [32].

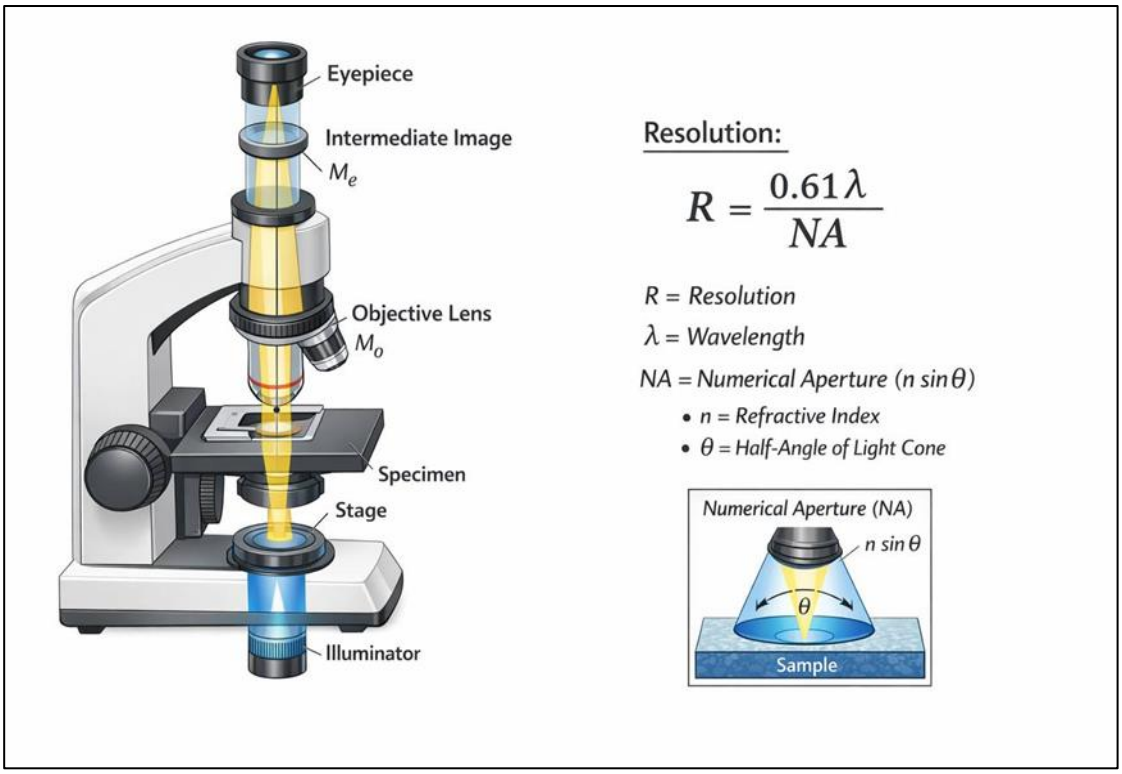
2.2 الخصائص المجهرية Microstructure Analysis

تشير إلى الصفات المرتبطة بالبنية الداخلية الدقيقة للمواد والتي يمكن ملاحظتها باستخدام المجاهر المختلفة مثل المجهر البصري والمجهر الإلكتروني.[32] وتشمل هذه الخصائص شكل الحبيبات، حجمها، توزيع الأطوار المختلفة، الحدود البلورية، إضافة إلى العيوب المجهرية مثل المسامية والانخلاعات. وتلعب الخصائص المجهرية دورًا مهمًا في تحديد السلوك الفيزيائي والميكانيكي للمواد، حيث تؤثر بشكل مباشر في متانتها، صلابتها، وقابليتها للتشوه. لذلك يُعد تحليل البنية المجهرية خطوة أساسية لفهم العلاقة بين تركيب المادة وخواصها المختلفة [33].

1.2.2 المجهر البصري Optical Microscope

يُعد المجهر البصري من أكثر الأدوات استخدامًا في دراسة المعادن والسيراميك، ويعتمد على انكسار وانعكاس الضوء لإظهار تضاريس السطح [34]. تُحدد القدرة التحليلية للمجهر بالعلاقة:

$$R = \frac{0.6\lambda}{NA} \qquad (1-2)$$

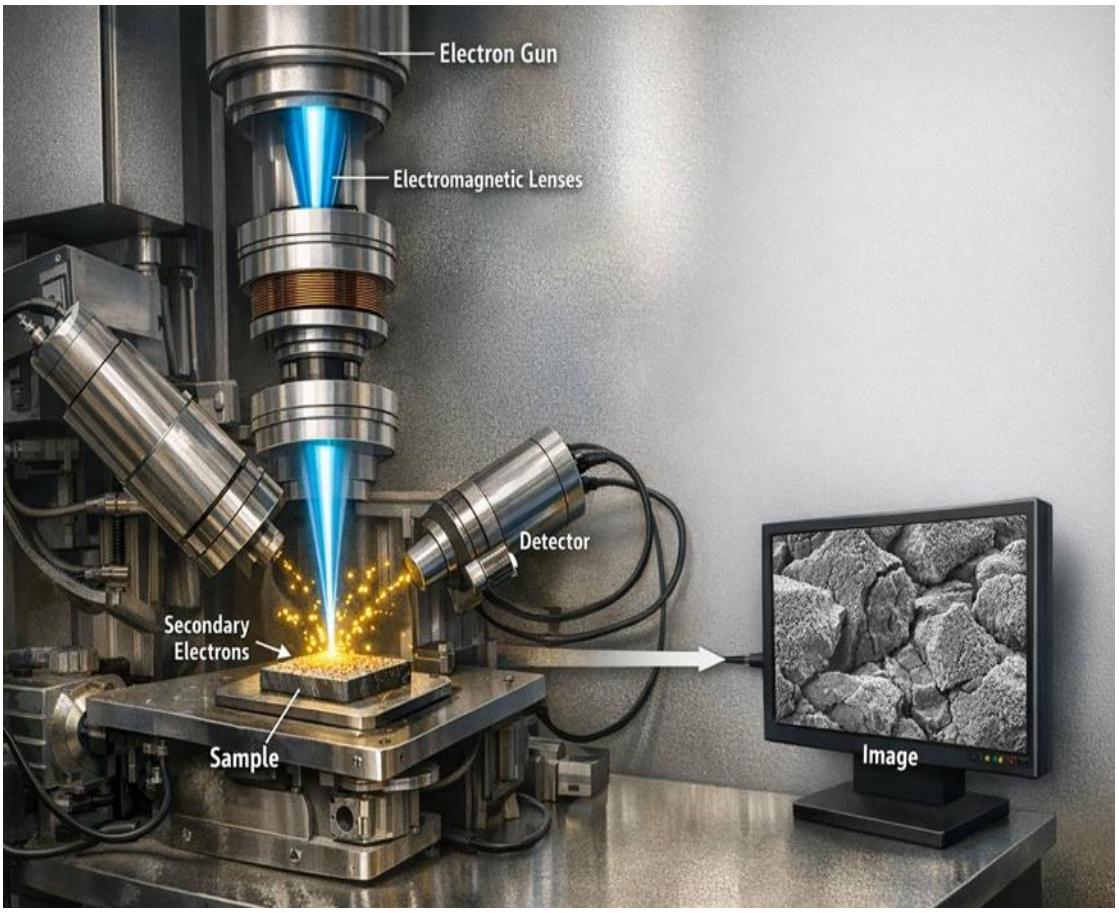


شكل (2–1) المجهر البصري.

معادلة (2–1) توضح ان الدقة تتحسن عند تقليل طول الموجة او زيادة الفتحة العددية [35]. ورغم محدوديته , فإنه يتيح قياس حجم الحبيبات ورؤية البنية الأولية للسطح بعد التلميع والصقل.

2.2.2 المجهر الالكتروني الماسح Scanner Electrical Microscope

يعتمد عمل المجهر الإلكتروني الماسح على تسليط حزمة من الالكترونات على العينة لتوليد إلكترونات ثانوية تُستخدم لتكوين صورة عالية الدقة [36]. يمتاز المجهر الإلكتروني الماسح بقدرة تحليلية تصل إلى 1–5 nm، مما يجعله أداة مثالية لدراسة الحبيبات الصغيرة [37].



شكل(2–2) المجهر الالكتروني الماسح.

3.2.2 قياس حجم الحبيبات ASTM E112

يعتمد التحليل العلمي الدقيق على تحويل البنى المعقدة إلى مؤشرات رقمية معيارية قابلة للمقارنة. في علم المواد، يُستخدم معيار ASTM E112 لتحديد متوسط حجم الحبيبات في المواد متعددة البلورات عبر العلاقة:

$$N = 2^{G-1} \qquad (2-2)$$

حيث ان:

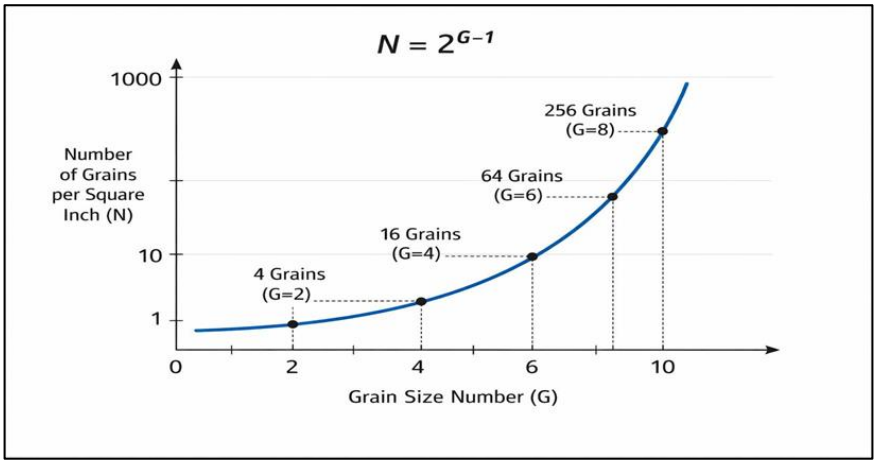
N= عدد الحبيبات ضمن بوصة مربعة عند تكبير ×100.

G= رقم حجم الحبيبات القياسي.

وتوضح هذه العلاقة أن زيادة وحدة واحدة في G تؤدي إلى تضاعف عدد الحبيبات تقريبًا، مما يعكس الطبيعة اللوغاريتمية للقياس البنيوي [38] أثبت العالم Hall (1951) أن تصغير حجم الحبيبات يؤدي إلى زيادة مقاومة الخضوع نتيجة إعاقة حدود الحبيبات لحركة الانخلاعات البلورية [39]، بينما قدّم العالم Petch (1953) الصياغة الرياضية التي تربط مقاومة المادة عكسيًا بجذر حجم الحبيبات [40]. وتؤكد المراجع القياسية في علم الميتالورجيا أن قياس حجم الحبيبات يمثل نموذجًا لتحويل البنية المجهرية إلى قيمة عددية معيارية تسمح بالمقارنة الموضوعية بين المواد المختلفة [41].

من الناحية المنهجية، يعكس هذا الأسلوب مبدأً علميًا عامًا يقوم على تحويل الخصائص البصرية إلى تمثيلات كمية قابلة للتحليل الإحصائي. وبالمثل، تعتمد أنظمة التعرف على الوجه المعتمدة على التعلم العميق على استخراج تمثيلات عددية (Feature Vectors) من الصور وتحويلها إلى فضاء رياضي عالي الأبعاد يمكن استخدامه في التمييز بين العينات الحقيقية. وهجمات التزوير. وعليه، فإن إدراج مفهوم القياس المعياري لحجم الحبيبات في هذا السياق يهدف

إلى إبراز أهمية القياس الكمي المنظم في تقييم الأنظمة المعقدة، سواء في تحليل البنى المجهرية أو في تقييم أداء نماذج كشف هجمات الـ spoofing.



شكل (2–3) العلاقة بين رقم حجم الحبيبة (G) وعدد الحبيبات في وحدة المساحة (N).

4.2.2 التحليل الإحصائي للصور وتقنيات تقدير العمق

يُستخدم التحليل الإحصائي للصور لاستخراج خصائص كمية مثل المسامية (Porosity) والنسب المئوية للمساحات المفتوحة ضمن المادة.

يُعبر عن المسامية بالمعادلة:

$$\textbf{Porosity}(\%) = \frac{\boldsymbol{A_{Void}}}{\boldsymbol{A_{attac}}} \times \mathbf{100} \qquad (\mathbf{3-2})$$

حيث:

- A_{total} = مساحة الفراغات أو العيوب داخل العينة
- A_{void} = المساحة الإجمالية للمنطقة المحللة [42]

توفر هذه الطريقة تقييمًا رقميًا دقيقًا للبنية المجهرية، وتُمكّن الباحث من مقارنة جودة العينات المختلفة بشكل موثوق علميًا [43].

5.2.2 تقنيات العمق التقليدية (Conventional Depth Sensing)

تهدف تقنيات العمق إلى تقدير المسافة بين أي نقطة في المشهد وجهاز الاستشعار، اعتمادًا على مبادئ هندسية أو زمنية ولها عدة فئات:

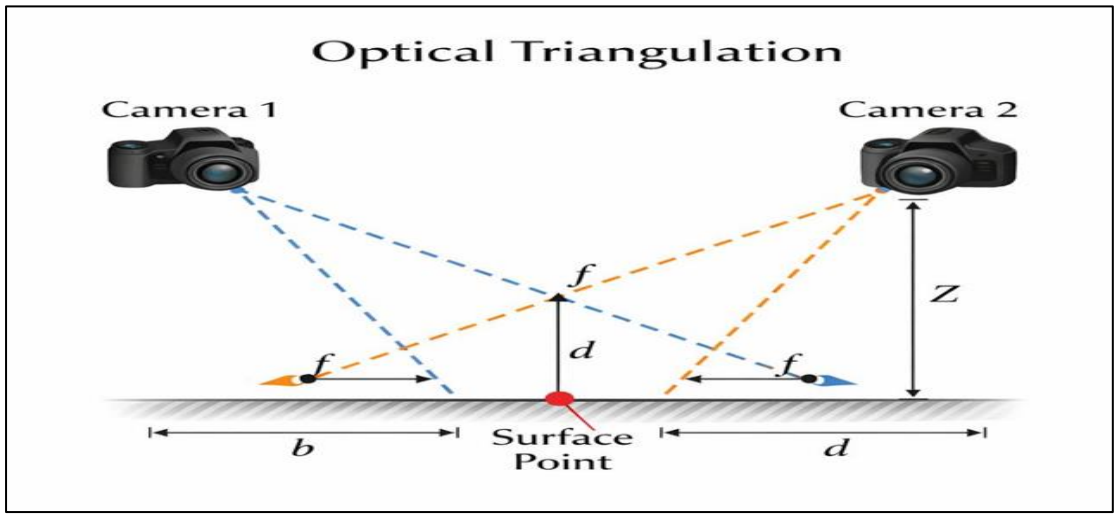
1. **التقنية المثلثية البصرية (Optical Triangulation)**

تعتمد على العلاقة الهندسية بين مصدر الضوء والكاميرا أو بين كاميرتين للحصول على عمق النقطة Z:

$$Z = \frac{b.f}{d} \qquad (4-2)$$

حيث:

- b = قاعدة القياس (Baseline) بين الكاميرات أو بين الكاميرا ومصدر الضوء
- f = البعد البؤري للكاميرا
- d = التباين بين الصورتين (Disparity) [44]



شكل (2-4) مبدأ التثليث البصري (Optical Triangulation) لتحديد موقع أو عمق نقطة على السطح باستخدام كاميرتين من زوايا مختلفة.

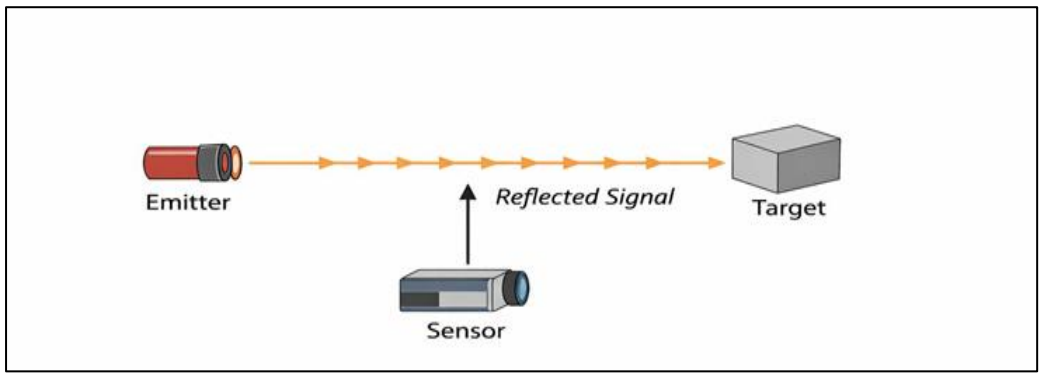
2. تقنية قياس العمق بالزمن Time of Flight (ToF)

تعتمد تقنية ToF على قياس الزمن الذي تستغرقه النبضة الضوئية للانتقال إلى الهدف والعودة إلى المستشعر، ويُحسب العمق وفق المعادلة:

$$d = \frac{ct}{2} \qquad (5-2)$$

حيث c سرعة الضوء و t زمن الرحلة الكلي [45].

تُستخدم هذه التقنية لإنتاج خرائط عمق مباشرة بدقة زمنية عالية، وتتميز بسرعة الاستجابة مقارنة بطرق الرؤية المجسمة [46]. إلا أن الأداء قد يتأثر بالضوضاء أو الانعكاسات المتعددة. تُعد تقنية ToF فعّالة في تطبيقات الرؤية الحاسوبية والأنظمة البيومترية، إذ توفر معلومات ثلاثية الأبعاد تساعد في التمييز بين الأجسام الحقيقية والصور ثنائية الأبعاد [47].



شكل(2-5) مبدأ قياس العمق بزمن الرحلة (Time of Flight – ToF)،

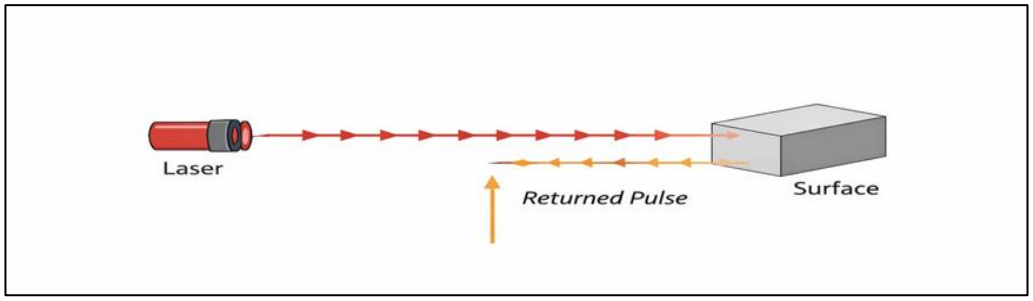
يمثل المبدأ الفيزيائي لتقنية زمن الرحلة (Time-of-Flight – ToF)، ومعناه كالتالي:

- Emitter (المرسل): يطلق نبضة ضوئية (عادةً ليزر أو أشعة تحت الحمراء).
- Target (الهدف): الجسم الذي تصطدم به النبضة.
- Reflected Signal (الإشارة المنعكسة): الضوء يرتد من سطح الهدف.
- Sensor (المستشعر): يستقبل الإشارة المرتدة ويقيس زمن الرحلة t.

ومن خلال قياس الزمن بين الإرسال والاستقبال نحسب المسافة باستخدام المعادلة (2-5)

3. تقنية المسح الليزري Laser Scanning

تقنية المسح الليزري تعتمد على نفس مبادئ Time-of-Flight (ToF)، لكنها تستخدم ليزر عالي الدقة لقياس العمق والمسافات بدقة أكبر مقارنة بالكاميرات التقليدية. في هذا النظام، يُرسل نبض ليزر نحو سطح الهدف، ثم يقيس المستشعر الزمن الذي تستغرقه النبضة للعودة حسب المعادلة (2-5). تستخدم هذه التقنية على نطاق واسع في الهندسة المعمارية، المسح الجغرافي، والمسح ثلاثي الأبعاد للوجه، حيث توفر نماذج ثلاثية الأبعاد دقيقة للغاية (49). كما أشارت الدراسات إلى أن المسح الليزري يتيح تمييز التفاصيل الدقيقة للسطح والملامح العميقة التي تكون مهمة في أنظمة التعرف على الوجه لكشف الهجمات الاحتيالية (50).



شكل (2-6) المسح الليزري.

يتم ارسال نبضة الليزر نحو السطح (Surface) وتقاس النبضة المرتدة بواسطة المستشعر لحساب العمق بدقة .

4. تقنية العمق من التركيز Depth from Focus

تعتمد أساليب العمق من التركيز على التقاط مجموعة صور عند مستويات تركيز مختلفة $z_1, z_2, \ldots, z_N$، ثم قياس درجة وضوح كل بكسل في كل صورة باستخدام دالة الحدة $S(x, y, z)$. بعد ذلك يُختار مستوى التركيز الذي يعطي أعلى قيمة للحدة لكل نقطة، وهذا المستوى يمثل عمق النقطة في المشهد [51]:

$$D(x, y) = \arg\max S(x,y,z) \qquad (2-6)$$

حيث:

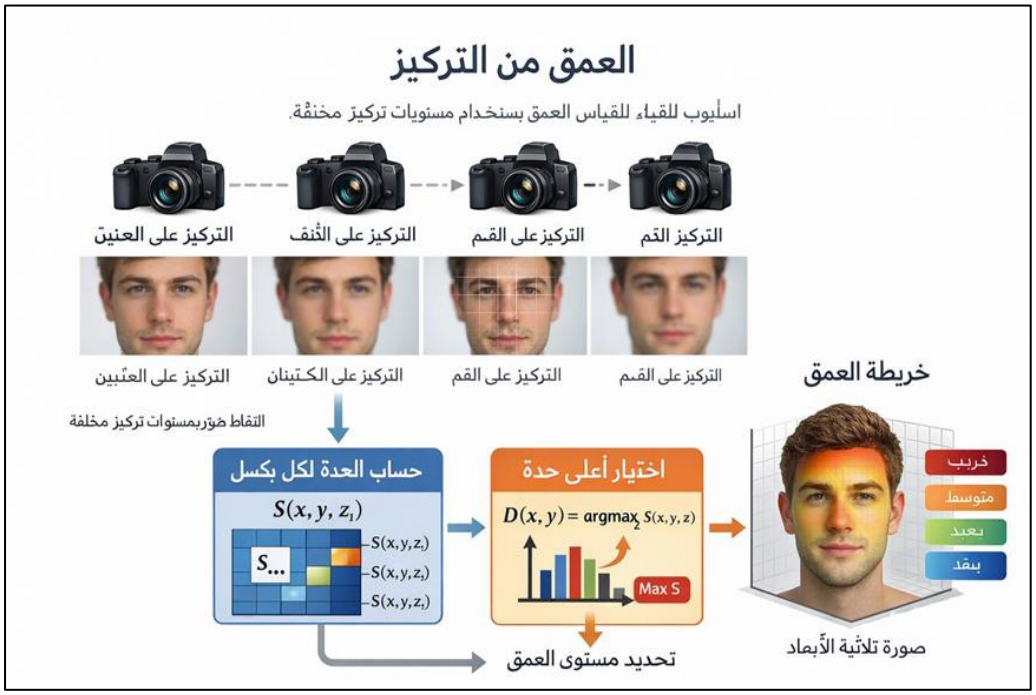
- (x, y) إحداثيات البكسل في الصورة،

- z مستوى التركيز،
- S(x, y, z) دالة الحدة (Sharpness Measure).

من أشهر دوال الحدة المستخدمة: Gradient-based measures مثل Laplacian وSobel، وFrequency-based measures مثل Tenengrad و Energy of High Frequencies، وMeasures تعتمد على التباين مثل Variance of Intensity [52].

تُجمع نتائج هذه الدوال عبر جميع مستويات التركيز، ثم يُختار المستوى الذي يعطي أعلى قيمة لكل بكسل لتكوين خريطة عمق ثلاثية الأبعاد D(x, y) [53].

تتميز هذه الطريقة بكونها منخفضة التكلفة وسهلة التطبيق مقارنة بأساليب الاستشعار الحديثة، وموثوقة عند وجود ضوء ثابت وعدم حركة سريعة في المشهد، لكنها أقل دقة في المشاهد منخفضة التباين أو عند وجود حركة [54].



شكل (2-7) يمثل العمق من التركيز.

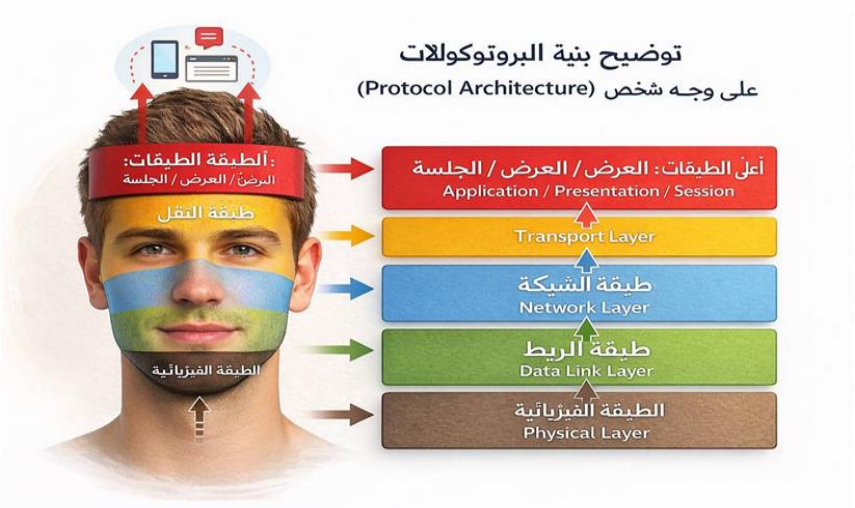
3.2 مجموعات البيانات القياسية Standard Datasets

تعد مجموعات البيانات القياسية حجر الأساس في تقييم أنظمة كشف هجمات العرض (Presentation Attack Detection — PAD)، إذ تعتمد معظم الدراسات على قواعد بيانات مرجعية لضمان قابلية المقارنة وإعادة إنتاج النتائج. في هذا القسم، نستعرض ثلاث قواعد بيانات شائعة الاستخدام في المجال مع تحليل نقدي لكل منها.

1.3.2 قاعدة بيانات وحدة المعالجة البصرية OULU–NPU

تم تقديم قاعدة بيانات OULU–NPU في عام 2017 من قبل Boulkenafet وآخرين [55]، بهدف توفير بيئة تقييم واقعية لأنظمة PAD على الأجهزة المحمولة. تحتوي القاعدة على 4950 مقطع فيديو لـ 55 مشاركًا، مسجلة عبر ثلاث جلسات مختلفة وباستخدام عدة هواتف ذكية، مما يسمح باختبار التعميم عبر تغيّر الجهاز والإضاءة والمشهد [55].

توفر هذه القاعدة أربعة بروتوكولات تقييم منظمة لاختبار التعميم عبر الأجهزة. (Generalization device) والتعميم عبر الإضاءة والمشهد والتعميم عبر الجلسات بحيث لا يتداخل نفس الشخص الجلسة بين المجموعتين والتعميم المشترك بين عدة عوامل تعتمد غالبية الدراسات التي تستخدم تقنية OULU–NPU على مقاييس APCER وBPCER وACER وفقًا لمعيار ISO/IEC 30107–3 [58]



شكل (2–8) بنية البروتوكولات.

وتمتاز قاعدة البيانات هذه بتصميم مخصّص للأجهزة المحمولة (قيمة عملية لتطبيقات الهاتف). بروتوكولات منسقة لفحص تعميم النماذج عبر ظروف متعددة.وبالرغم من أهميتها في تقييم التعميم عبر الأجهزة، فإن عدد المشاركين (55) يظل محدودًا نسبيًا، كما أن تركيزها الأساسي على هجمات العرض الثنائية الأبعاد قد لا يغطي التهديدات ثلاثية الأبعاد الحديثة [55].

CASIA–FASD 2.3.2

تم تقديم قاعدة CASIA–FASD بواسطة Zhang وآخرين عام 2012 [56]، وتُعد من أوائل قواعد البيانات المنظمة في مجال كشف التزييف الوجهي. تتضمن القاعدة عدة أنواع من الهجمات، منها الصور المطبوعة المسطحة، والصور المطبوعة مع فتحات للعين (cut–eye attacks)، إضافة إلى هجمات إعادة العرض [56] (video replay). كما تم تسجيل البيانات باستخدام كاميرات بدقات مختلفة، مما يتيح دراسة تأثير جودة الالتقاط على أداء أنظمة PAD [56] وعلى الرغم من تنوع أنواع الهجمات، فإن التسجيل تم في بيئات مخبرية محكومة نسبيًا، مما قد يحد من قابلية تعميم النتائج على البيئات الواقعية غير المتحكم بها [56].

Replay–Attack Database 3.3.2 قاعدة بيانات لهجمات إعادة الارسال

تم تطوير قاعدة Replay-Attack في Idiap Research Institute، وقد تم تقديمها رسميًا في عام 2012 [57]. تحتوي القاعدة على حوالي 1300 مقطع فيديو لـ 50 مشاركًا، وتشمل هجمات الطباعة وإعادة العرض بالفيديو تحت ظروف إضاءة مختلفة [57]. توفر القاعدة تقسيمًا منهجيًا إلى مجموعات تدريب وتطوير واختبار، مما جعلها معيارًا مرجعيًا في الدراسات المبكرة في المجال [57].

بالرغم من أهميتها الا ان هذه القاعدة تركز على الهجمات الثنائية الأبعاد فقط (print & replay)، ولا تتضمن هجمات الأقنعة ثلاثية الأبعاد أو الهجمات المتقدمة، مما يحد من تمثيلها للسيناريوهات الحديثة [57].

4.3.2 مقياس او معيار التقييم القياسي Standard Evaluation Metric

ويستخدم لقياس أداء شيء معين حتى نستطيع المقارنة بين النتائج تعتمد معظم الدراسات الحديثة في تقييم أنظمة PAD على التعريفات الرسمية الواردة في معيار [58]، والذي يحدد مقاييس الأداء التالية:

Attack Presentation Classification Error Rate (APCER):
APCER = N_attack→bona_fide / N_attack

Bona Fide Presentation Classification Error Rate (BPCER):
BPCER = N_bona_fide→attack / N_bona_fide

Average Classification Error Rate (ACER):
ACER = (APCER + BPCER) / 2

كما يوصي المعيار في بعض الحالات باحتساب APCER لكل فئة PAI واختيار أعلى قيمة (worst-case PAI) لتوفير تقييم أكثر تحفظًا [58].

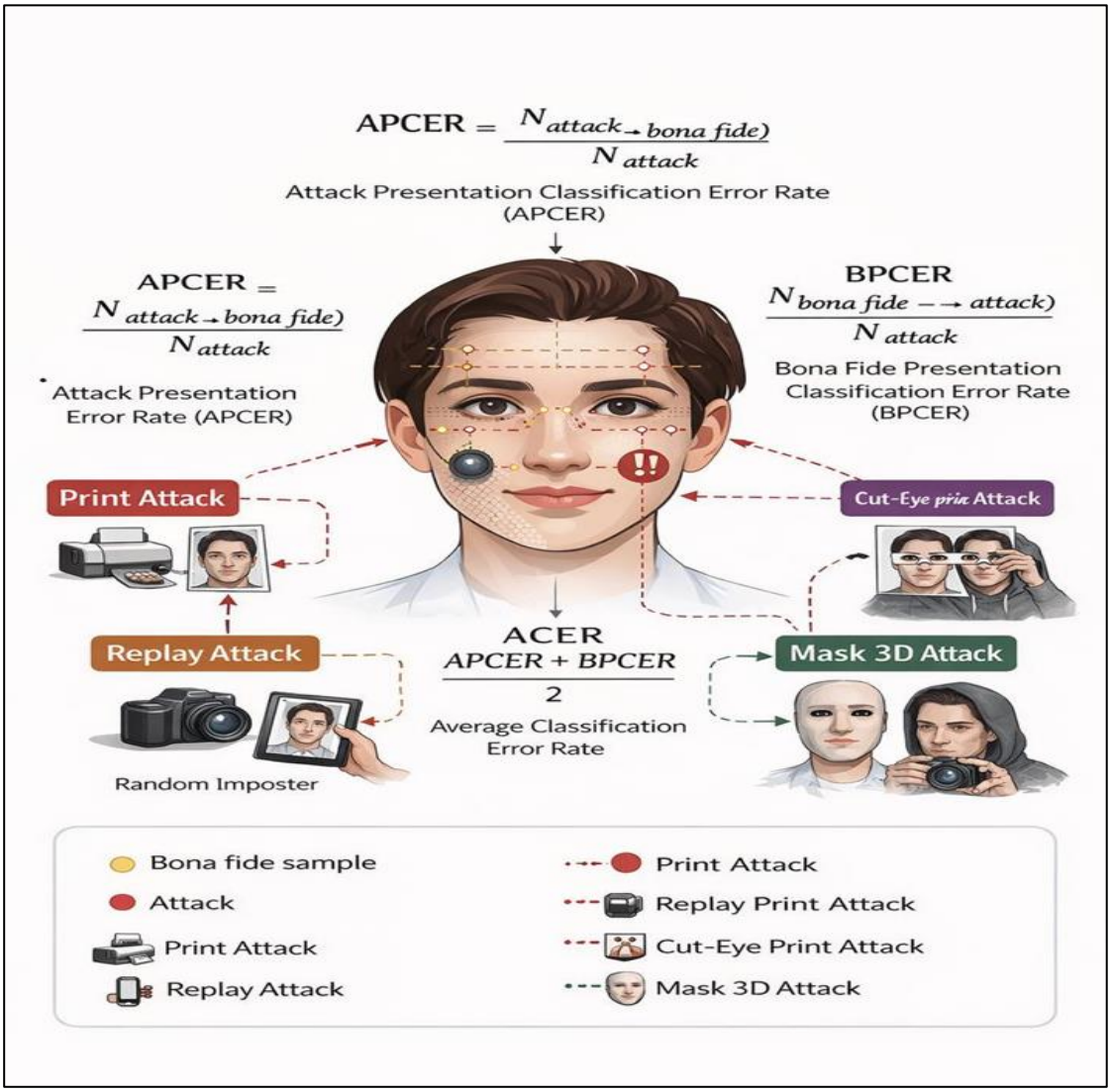
4.2 مقارنة مُركّزة بين الثلاث قواعد (تلخيص نقدي)

Dataset	subjects	videos	Attack Types	Key Focus	Ref.
OULU-NPU	55	4950	Print & Replay (2D)	Cross-device& cross-session evaluation	55
CASIA FASD	50	~600	Print (flat, cut- + photo) Reply	Multiple attack styles	56
Replay-Attack	50	~1300	Print & Replay (2D)	Structured train/dev/ test	57

يتضح من الجدول اعلاه أن قواعد البيانات الثلاث تشترك في تركيزها على هجمات العرض الثنائية الأبعاد (2D Presentation Attacks)، مما يعكس طبيعة التهديدات السائدة في فترة

تطويرها. إلا أن هذا التركيز يُعد قيدًا عند تقييم الأنظمة الحديثة المصممة لمواجهة هجمات الأقنعة ثلاثية الأبعاد أو الهجمات المتقدمة [55,57].

تتميز OULU-NPU بتركيزها على تعميم الأداء عبر الأجهزة المحمولة والجلسات المختلفة[55] ، وهو ما يجعلها أكثر ملاءمة لتقييم التطبيقات الواقعية مقارنةً بـ CASIA-FASD [56] و[57] Replay-Attack اللتين تم تسجيلهما في بيئات مخبرية محكومة نسبيًا. من ناحية مقاييس التقييم، تعتمد الدراسات التي تستخدم هذه القواعد عادةً على تعريفات ISO/IEC30107- لضمان توحيد آلية الإبلاغ عن النتائج [58].



شكل (2-9) انواع هجمات الوجه في أنظمة كشف الهجمات الحيوية مع مقاييس.

الفصل الثالث

مقارنة بين اشهر الخوارزميات

1.3 المقدمة Introduction

تعد تقنيات التعرف على الوجه من أبرز تطبيقات القياسات الحيوية، إذ تعتمد على تحليل السمات المورفولوجية للوجه وتحويلها إلى تمثيل عددي يمكن مقارنته رياضيًا داخل فضاء سماتي مخصص. وقد شكّلت هذه التقنيات محور اهتمام واسع في مجالات الأمن، والتحقق من الهوية، والأنظمة الذكية، نظرًا لقدرتها على توفير آلية غير تلامسية للتعرّف البيومتري [59]. في المراحل الأولى من تطور هذا المجال، اعتمدت الأنظمة على أساليب إحصائية خطية، ومن أبرزها طريقة Eigen-faces القائمة على تحليل المركبات الرئيسية (PCA)، والتي تسمح بإسقاط بيانات الصور في فضاء منخفض الأبعاد مع الاحتفاظ بأكبر قدر ممكن من التباين [60]. وعلى الرغم من كفاءتها الحسابية وسهولة تطبيقها، إلا أنها تعاني من حساسية واضحة لتغيرات الإضاءة، ووضعية الرأس، وتعابير الوجه، مما يحد من قدرتها على التعميم في البيئات الواقعية غير المضبوطة.

لاحقًا، ظهرت خوارزميات قائمة على تحليل النسيج المحلي مثل Local Binary Patterns (LBP)، والتي حسّنت مقاومة النظام لتغيرات الإضاءة مقارنة بالطرق الخطية التقليدية [61]. ومع ذلك، فإن اعتمادها على خصائص مصممة يدويًا (Handcrafted Features) يجعل قدرتها محدودة في تمثيل العلاقات غير الخطية المعقدة للسمات الوجهية، خاصة عند التعامل مع قواعد بيانات كبيرة ومتنوعة. مع ظهور التعلم العميق، أحدثت الشبكات العصبية الالتفافية (CNN) تحولًا جوهريًا في تقنيات التعرف على الوجه، إذ أصبحت قادرة على تعلم السمات تلقائيًا من البيانات الخام دون تدخل يدوي في مرحلة استخراج الخصائص. وقد أظهرت نماذج مثل DeepFace تقاربًا كبيرًا مع الأداء البشري في مهام التحقق من الهوية [62]، في حين قدّم نموذج Face-Net إطارًا موحدًا لتعلم تمثيل متجهي مضغوط للوجه باستخدام أسلوب Triplet Loss، محققًا دقة عالية جدًا في قواعد البيانات القياسية [63]. على الرغم من هذه القفزة النوعية في مستوى الدقة، إلا أن

النماذج العميقة غالبًا ما تتطلب موارد حاسوبية كبيرة وزمن تدريب طويل، كما قد تتأثر بانحياز بيانات التدريب وعدم توازنها. لذلك، فإن المقارنة بين أشهر الخوارزميات يجب أن تتجاوز معيار الدقة لتشمل الكفاءة الحسابية، وقابلية التعميم، والاستقرار تحت ظروف تصوير مختلفة، ومتطلبات العتاد. ويُعد هذا التحليل المقارن خطوة أساسية لاختيار النموذج الأنسب وفقًا لطبيعة التطبيق والقيود العملية المفروضة عليه.

2.3 اشهر الخوارزميات المستخدمة في تقنيات التعرف على الوجه

تشمل خوارزميات التعرف على الوجه عدة أساليب أساسية، منها خوارزمية Eigenfaces التي تعتمد على تحليل المكونات الرئيسية (PCA) لاستخراج السمات المميزة للوجه، مما يقلل الأبعاد ويزيد سرعة المقارنة. وهناك Fisherfaces التي تستخدم تحليل التمييز الخطي (LDA) لتحسين التفريق بين الوجوه المشابهة. بالإضافة إلى ذلك، خوارزميات LBPH (Local Binary Patterns Histograms) تركز على القوام المحلي للوجه، وهي قوية أمام اختلاف الإضاءة. أما الأساليب الحديثة، فتشمل الشبكات العصبية العميقة مثل CNNs، التي تتعلم التمثيلات المميزة مباشرة من الصور، مما يزيد الدقة في التعرف على الوجوه حتى في ظروف معقدة. كل خوارزمية لها مميزاتها وقيودها، حيث تعتمد الأداء على جودة البيانات والإضاءة وزوايا التصوير ومن اشهر الخوارزميات:

1.2.3 خوارزمية Eigen-faces (PCA)

تعتمد على تحليل المكونات الرئيسية (PCA) لاستخراج أهم السمات الخطية التي تمثل الوجه وتقليل الأبعاد [64].

آلية العمل

1. تحويل صور الوجوه إلى متجهات.
2. حساب متوسط الوجه.
3. استخراج المتجهات الذاتية (Eigenvectors).

4. إسقاط الصورة الجديدة على فضاء الوجوه (Face Space) والمقارنة باستخدام مسافة إقليدية [64].

المزايا

- تقليل الأبعاد بكفاءة.
- سرعة تنفيذ عالية.

العيوب

- حساسة للإضاءة والتعبيرات.
- تعتمد على تمثيل خطي فقط [64].

2.2.3 خوارزمية Fisher-faces (LDA)

تعتمد على التحليل التمييزي الخطي (LDA) لزيادة التباين بين الفئات وتقليل التباين داخل الفئة الواحدة [65].

آلية العمل

1. تقليل الأبعاد باستخدام PCA أولاً.
2. تطبيق LDA لتعظيم الفصل بين الأشخاص المختلفين.
3. التصنيف باستخدام أقرب مسافة [65].

المزايا

- أداء أفضل في ظروف الإضاءة المختلفة.
- قدرة أعلى على التمييز بين الأفراد.

العيوب

• تحتاج بيانات تدريب ممثلة جيداً لكل فئة.

• أقل كفاءة مع عدد كبير جداً من الفئات [65].

3.2.3 خوارزمية Local Binary Patterns Histograms (LBPH)

تعتمد على استخراج الخصائص النسيجية من الصورة باستخدام الأنماط الثنائية المحلية [66].

آلية العمل

1. تقسيم الصورة إلى مناطق.
2. تطبيق LBP لكل بكسل.
3. حساب المدرج التكراري لكل منطقة.
4. مقارنة المدرجات باستخدام مسافة تشي–تربيع [66].

المزايا

• مقاومة نسبية لتغير الإضاءة.

• مناسبة للأنظمة الزمن الحقيقي.

العيوب

• أقل دقة من الطرق العميقة.

• تعتمد على الخصائص اليدوية (Handcrafted features) [66].

4.2.3 CNNs (Convolutional Neural Networks – الشبكات العصبية التلافيفية)

تعتمد CNNs على هيكل شبكي متعدد الطبقات يقوم باستخراج الميزات من الصور تلقائيًا بترتيب هرمي من الطبقات البسيطة إلى الطبقات عالية المستوى، ومن ثم يستخدم هذه الميزات للتصنيف أو التحقق من الهوية [67].

المميزات:

• قوية في التعامل مع الصور عندما تكون الظروف جيدة، وتحقق دقة عالية عند التدريب على مجموعات بيانات كبيرة [67].

• قادرة على استخراج ميزات متعددة المستويات من الوجه بدون الحاجة لاستخراج ميزات يدوية [68].

العيوب:

• تتطلب بيانات ضخمة ومتنوعة للحصول على أداء قوي، وإلا ستظهر فجوات خاصة بين الأعراق المختلفة [69].

• الأداء يتأثر بالإضاءة الضعيفة والزوايا الجانبية وتغطية أجزاء الوجه [69].

• تحتاج موارد حسابية كبيرة أثناء التدريب والتطبيق في الوقت الحقيقي [67].

5.2.3 FaceNet (Embedding + Triplet Loss)

يحول FaceNet كل وجه إلى تمثيل رقمي في فضاء متجهي (embedding) بحيث تكون المسافات بين التمثيلات تمثل درجة التشابه، ويستخدم Triplet Loss لتقليل المسافة بين تمثيلات نفس الشخص وزيادة المسافة بين تمثيلات أشخاص مختلفين [70].

المميزات:

• يقدم دقة عالية جدًا على بيانات كبيرة مثل LFW [70].

• إنتاج تمثيل رقمي صغير الحجم (byte-128) يسمح بمقارنات سريعة للتطبيقات واسعة النطاق [71].

• مرن في التطبيقات التي تحتاج تمييز وجوه متعددة أو التحقق من الهوية والتجميع دون إنشاء نموذج تصنيف صريح [71].

العيوب:

• قد يتراجع الأداء في ظروف الإضاءة السيئة أو الزوايا الحادة إذا لم يتم التدريب عليها جيدًا [72].

• عملية mining لـ triplets أثناء التدريب معقدة وتزيد من تعقيد التدريب [72].

• أداء أقل توازنًا في التعرف العرقي إذا كانت البيانات غير ممثلة لجميع المجموعات [72].

6.2.3 ArcFace (Additive Angular Margin Loss)

طريقة العمل

ArcFace هو تحسين على هيكل CNN مع إضافة "angular margin" في دالة الخسارة بحيث تُعظم المسافة الزاويّة بين تمثيلات الوجوه المختلفة وتُقلل داخل نفس هوية الوجه [73].

المميزات:

• يحقق تمييزًا أقوى للهويات المختلفة عن FaceNet بسبب إضافة هامش زاوي في التدريب [73].

• أداء ممتاز على مجموعات بيانات كبيرة، ويحقق دقة ممتازة في البيئات القياسية [74].

• يوازن بين الدقة والكفاءة الحسابية مقارنة ببعض نماذج CNN الأعمق بكثير [74].

العيوب:

• لا يقضي التحيّز العرقي تمامًا إذا كانت بيانات التدريب غير متوازنة [75].

• أكثر تعقيدًا في التنفيذ بسبب إعدادات هامش الزاوية والإجراءات الحسابية [73].

• الأداء في الحالات الواقعية قد لا يكون أفضل بشكل واضح من FaceNet إذا لم يتدرب النموذج على هذه السيناريوهات [75].

3.3 اهم التحديات في خوارزمية التعرف على الوجه في التعلم العميق من حيث التمييز العرقي

تقنيات التعرف على الوجه باستخدام التعلم العميق أثبتت كفاءتها العالية في العديد من التطبيقات، إلا أنها تواجه تحديات مهمة فيما يتعلق بالتمييز العرقي، والذي غالبًا ما يظهر بسبب اختلاف لون البشرة والتنوع العرقي بين المجموعات السكانية. أحد أبرز هذه التحديات هو اختلال بيانات التدريب، حيث تميل مجموعات البيانات المتاحة إلى تمثيل وجوه بيضاء أكثر من وجوه أصحاب البشرة الداكنة أو الأعراق الأخرى، ما يجعل الشبكات العصبية تتعلم تمثيلات وجه أدق للأعراق المهيمنة وتفشل نسبيًا في التعرف على وجوه غير ممثلة بشكل كافٍ في التدريب [76]. هذا الاختلال يؤدي إلى تفاوت واضح في معدلات الخطأ بين الأعراق، إذ يظهر النظام أداءً ممتازًا على وجوه بيضاء، بينما ترتفع معدلات الخطأ عند التعرف على وجوه سوداء أو آسيوية [77].

بالإضافة لذلك، تمثيل الميزات في الشبكات العميقة يمكن أن يكون متحيزًا، إذ تتعلم النماذج السمات الأكثر شيوعًا في البيانات، مما يقلل قدرتها على استخراج الخصائص المميزة للأعراق الأخرى، ويزيد من فجوات الأداء العرقي [77]. كما يمكن أن يتداخل هذا التحيز مع عوامل ديموغرافية أخرى مثل الجنس والعمر، حيث أظهرت الدراسات ضعف أداء النماذج عند النساء ذوات البشرة الداكنة مقارنة بغيرهن [76]. علاوة على ذلك، محدودية مجموعات البيانات القياسية

تجعل تقييم أداء النماذج غير كافٍ، إذ قد تبدو النماذج دقيقة عند اختبارها على بيانات ممثلة، لكنها تفشل عند التعرض لأعراق متنوعة وظروف تصوير مختلفة [76].

هذه التحديات توضح الحاجة إلى تصميم مجموعات بيانات أكثر تنوعًا واستراتيجيات تدريب تقلل من التحيز العرقي دون التضحية بالدقة العامة، مثل استخدام بطاقات التعلم العميق العادلة أو تعديل دوال الخسارة لتوازن التمثيلات العرقية، لضمان أن الخوارزميات تكون فعّالة لجميع الفئات العرقية بشكل عادل [77].

4.3 النقد البناء لكل خوارزمية

1.4.3 CNNs (شبكات الالتفاف العصبية)

الإيجابيات:

1. دقيقة جداً على الوجوه الممثلة جيداً في البيانات [78].
2. فعّالة في استخراج الميزات الأساسية مثل شكل العيون، الأنف، والفم [78].

النقد البنّاء:

1. تعاني من تحيز عرقي إذا كانت البيانات غير متوازنة، حيث تقل دقتها على وجوه أعراق أقل تمثيلاً [79].

تتأثر بالظروف غير المثالية مثل الإضاءة السيئة أو الزوايا الجانبية، مما يزيد فجوة الأداء بين الأعراق [79].

2.4.3 FaceNet (Embedding + المسافة الكونية)

الإيجابيات:

1. ممتازة لتمييز الهوية حتى بين ملايين الصور [80].

2. سهلة الاستخدام مع تقنيات البحث عن الأقرب (nearest neighbor) باستخدام الـ embeddings [80].

النقد البنّاء:

1. دقتها العرقية غير متوازنة إذا كانت بيانات التدريب منحازة، مما يؤدي إلى زيادة الأخطاء عند بعض الأعراق [81].
2. نموذج "صندوق أسود"، صعب تفسير سبب الخطأ العرقي أو تصحيحه بدون بيانات جديدة متنوعة [81].

3.4.3 ArcFace (تحسين المسافة الزاويّة)

الإيجابيات:

1. تقلل الأخطاء الناتجة عن اختلاف الإضاءة أو الزوايا مقارنة بـ FaceNet [82].
2. تحسن فصل الهويات المختلفة في فضاء الـ embedding، ما يزيد الدقة العامة [82].

النقد البنّاء:

1. دقتها العرقية لا تزال تعتمد على توازن بيانات التدريب، فإذا كانت البيانات منحازة فإن أداء النموذج يختلف بين الأعراق [83].
2. تحتاج لمجموعات بيانات كبيرة ومتنوعة لتحقيق العدالة العرقية، وإلا تستمر الفجوات [83].

الخلاصة البنّاءة:

a. كل خوارزمية لها قوتها الخاصة، لكنها تعاني من تحيز عرقي إذا لم يتم تدريبها على بيانات متنوعة [84].
b. حتى ArcFace الأكثر تطوراً يحتاج لمراجعة البيانات والتدريب المستمر لتقليل الفجوة بين الأعراق [84].

الفصل الرابع

النتائج التي توصل لها الباحثون

استخدام طريقة التعلم العميق في كشف تزوير هوية الوجه أدى إلى نتائج مهمة ومتقدمة في العديد من المجالات البحثية والتطبيقية [41]. فيما يلي أبرز النتائج التي توصل إليها الباحثون من خلال استخدام هذه الطريقة:

1.4 ما توصل إليه الباحثون (Findings of Previous Studies)

1. توصل الباحثون إلى أن تقنيات التعلم العميق، خصوصاً الشبكات العصبية الالتفافية، حققت تفوقاً ملحوظاً في كشف هجمات تزوير الهوية مقارنة بالأساليب التقليدية [85].
2. بيّنت الدراسات أن أنظمة التعرف على الوجه لا تزال عرضة لهجمات متعددة، مثل هجمات الصور الثابتة والفيديوهات المعاد عرضها، إضافة إلى الأقنعة ثلاثية الأبعاد [86].
3. أظهرت الأبحاث أن دمج نماذج متعددة مثل CNN وTransformers يؤدي إلى تحسين الأداء وزيادة دقة الكشف عن التزوير [87].
4. أكد الباحثون أن تنوع بيانات التدريب يلعب دوراً أساسياً في تحسين قدرة النماذج على التعميم واكتشاف الهجمات الجديدة [88].
5. توصلت الدراسات إلى أن مشكلة التعميم عبر المجالات (Domain Generalization) تمثل تحدياً رئيسياً يؤثر على كفاءة النماذج في البيئات المختلفة [89].
6. أثبتت الأبحاث أن استخدام تقنيات متعددة الوسائط، مثل دمج بيانات RGB مع العمق أو الأشعة تحت الحمراء، يحسن من قدرة الأنظمة على كشف التزوير [90].
7. بيّنت الدراسات أن استخدام تقنيات الإشراف المتقدم، مثل خرائط العمق الزائفة والإشراف الزمني، يعزز من دقة التمييز بين الوجه الحقيقي والمزيف [91].
8. توصل الباحثون إلى أن تحليل الخصائص الفيزيائية، مثل الملمس والإضاءة والتغيرات الحيوية في الوجه، يسهم بشكل فعال في كشف التزوير [92].

9. أظهرت النتائج أن الهجمات التوليدية (Deepfake) تمثل تحدياً متزايداً بسبب ارتفاع مستوى واقعيتها [93].
10. أكدت الدراسات أن النماذج الحالية تعاني من ضعف في اكتشاف الهجمات غير المعروفة (Zero-shot attacks) [94].
11. بيّنت الأبحاث أن النماذج الخفيفة مثل MobileNet توفر حلولاً فعالة للتطبيقات العملية مع الحفاظ على كفاءة الأداء [95].
12. توصل الباحثون إلى أن الأنظمة متعددة الطبقات أكثر فعالية في مواجهة أنواع الهجمات المختلفة مقارنة بالأنظمة الأحادية [96].
13. أكدت الدراسات أهمية استخدام معايير تقييم متعددة مثل FAR وFRR وHTER للحصول على تقييم دقيق لأداء الأنظمة [97].
14. أظهرت الأبحاث أن دمج التحليل المكاني والزماني يحسن من كشف الهجمات الديناميكية مثل إعادة عرض الفيديو [98].
15. توصل الباحثون إلى أن تطور تقنيات التزييف العميق يتطلب تحديثاً مستمراً لنماذج الكشف لمواكبة هذه التطورات [99].
16. بيّنت الدراسات أن قابلية تفسير النماذج تمثل تحدياً مهماً في تطبيقات الأمن والأنظمة الحساسة [100].
17. أكدت الأبحاث ضرورة تطوير قواعد بيانات أكثر تنوعاً وواقعية لتحسين أداء نماذج كشف التزوير [101].
18. توصل الباحثون إلى أن نجاح أنظمة كشف التزوير يعتمد على تكامل عدة عوامل تشمل البيانات، الخوارزميات، وأجهزة الاستشعار [102].

2.4 الفجوة البحثية (Research Gap)

1. على الرغم من التقدم الكبير في تقنيات التعلم العميق، لا تزال النماذج الحالية تعاني من ضعف في التعميم عند تطبيقها على بيانات من بيئات مختلفة أو غير مألوفة [89]
2. معظم الدراسات ركزت على هجمات معروفة ومحددة، بينما لا تزال قدرة الأنظمة على اكتشاف الهجمات غير المعروفة (Zero-shot attacks) محدودة [94].
3. هناك نقص واضح في قواعد البيانات الواقعية التي تعكس ظروف الاستخدام الحقيقية، مثل تغيّر الإضاءة وزوايا التصوير وتنوع الأجهزة [103].
4. بالرغم من تطور تقنيات التزييف العميق (Deepfake)، فإن العديد من نماذج الكشف الحالية غير قادرة على مواكبة هذا التطور السريع [93]، [104].
5. تعتمد أغلب الأنظمة على بيانات أحادية (RGB فقط)، مع قلة في الأبحاث التي تستثمر بشكل كافٍ في الأنظمة متعددة الوسائط [105].
6. لا تزال قابلية تفسير نماذج التعلم العميق محدودة، مما يعيق استخدامها في التطبيقات الحساسة التي تتطلب شفافية في اتخاذ القرار [106].
7. تفتقر العديد من الدراسات إلى تقييم شامل باستخدام قواعد بيانات متعددة، مما يؤدي إلى نتائج قد لا تعكس الأداء الحقيقي للنماذج [107].
8. هناك حاجة إلى نماذج أكثر كفاءة من حيث استهلاك الموارد لتناسب التطبيقات الواقعية، خصوصاً في الأجهزة المحمولة [108].

3.4 التوصيات (Recommendations)

1. تطوير نماذج تعتمد على تقنيات التعميم عبر المجالات (Domain Generalization) لتحسين الأداء في بيئات مختلفة [89].
2. التركيز على تصميم أنظمة قادرة على اكتشاف الهجمات غير المعروفة باستخدام تقنيات التعلم بدون إشراف أو التعلم المستمر [94].
3. إنشاء قواعد بيانات جديدة أكثر تنوعاً وواقعية تشمل مختلف أنواع الهجمات وظروف التصوير [109].
4. دمج تقنيات متعددة الوسائط (مثل RGB + Depth + IR) لزيادة موثوقية أنظمة كشف التزوير [110].
5. تطوير خوارزميات قادرة على مواكبة تطور تقنيات التزييف العميق وتحليلها بشكل أكثر دقة [93]، [99].
6. تعزيز قابلية تفسير النماذج باستخدام تقنيات الذكاء الاصطناعي التفسيري (Explainable AI) لزيادة الثقة في الأنظمة [111]
7. اعتماد بروتوكولات تقييم أكثر صرامة تشمل الاختبار عبر قواعد بيانات مختلفة للحصول على نتائج أكثر واقعية [97].
8. تصميم نماذج خفيفة وفعالة يمكن تطبيقها على الأجهزة المحمولة دون التأثير على الأداء [95].
9. استخدام أنظمة متعددة الطبقات تجمع بين أكثر من تقنية للكشف عن التزوير بدلاً من الاعتماد على نموذج واحد [96].
10. دمج التحليل المكاني والزماني والإشارات الحيوية لتحسين دقة الكشف في السيناريوهات الواقعية [92]، [98].

الفصل الخامس

الاستنتاجات التي سيتم استنباطها من البحث والاعمال المستقبلية المقترحة ضمن هذا المجال

1.5 الاستنتاجات Conclusions

1. تُظهر الدراسات الحديثة أن نماذج التعلم العميق، خصوصاً الشبكات العصبية الالتفافية، تحقق أداءً متقدماً في كشف هجمات تزوير الهوية مقارنة بالأساليب التقليدية المعتمدة على الخصائص اليدوية [112].
2. لا تزال أنظمة التعرف على الوجه عرضة لأنواع متعددة من الهجمات، بما في ذلك الصور المطبوعة، إعادة عرض الفيديو، الأقنعة ثلاثية الأبعاد، والهجمات التوليدية (Deepfake) [113].
3. أثبتت النماذج الهجينة التي تجمع بين CNN وTransformer قدرتها على تحسين دقة الكشف من خلال الاستفادة من الخصائص المكانية والزمانية معاً [114].
4. تعتمد فعالية أنظمة كشف التزوير بشكل كبير على تنوع وجودة بيانات التدريب، حيث يؤدي نقص البيانات إلى ضعف التعميم على الهجمات الجديدة [115].
5. تمثل مشكلة التعميم عبر المجالات (Domain Generalization) تحدياً رئيسياً، إذ أن النماذج غالباً ما تفشل عند اختبارها على قواعد بيانات مختلفة [116].
6. أظهرت الأنظمة متعددة الوسائط (Multimodal) التي تدمج RGB مع العمق أو الأشعة تحت الحمراء أداءً أفضل مقارنة بالأنظمة أحادية المصدر [117].
7. تلعب تقنيات الإشراف المتقدم، مثل خرائط العمق الزائفة والإشراف الزمني، دوراً مهماً في تحسين التمييز بين الوجوه الحقيقية والمزيفة [118].

8. يساهم تحليل الخصائص الفيزيائية مثل الملمس، الإضاءة، والإشارات الحيوية (rPPG) في تعزيز دقة أنظمة كشف التزوير [119].
9. لا تزال الأنظمة الحالية تواجه تحديات كبيرة في كشف الهجمات التوليدية الحديثة ذات الواقعية العالية [120].
10. تُعد الهجمات غير المعروفة (Zero-shot attacks) من أبرز التحديات التي تتطلب تطوير نماذج قادرة على التعميم واكتشاف أنماط جديدة [121].
11. توفر النماذج الخفيفة (Lightweight Models) حلولاً فعالة للتطبيقات الواقعية، خاصة في الأجهزة المحمولة، مع الحفاظ على توازن بين الدقة والكفاءة [122].
12. أظهرت الدراسات أن الأنظمة متعددة الطبقات (Multi-layered Systems) أكثر كفاءة في مواجهة أنواع الهجمات المختلفة مقارنة بالأنظمة الأحادية [123].
13. تلعب معايير التقييم مثل FAR وFRR وHTER دوراً أساسياً في تقييم أداء الأنظمة، خاصة عند الاختبار عبر قواعد بيانات مختلفة [124].
14. يساهم دمج التحليل المكاني (Spatial) والزماني (Temporal) في تحسين قدرة الأنظمة على كشف الهجمات الديناميكية [125].
15. يتسارع تطور تقنيات التزييف العميق، مما يفرض الحاجة إلى تحديث مستمر لنماذج الكشف لمواكبة هذا التطور [126].
16. تُعد قابلية تفسير نماذج التعلم العميق من التحديات المهمة، خاصة في التطبيقات الأمنية الحساسة [127].
17. هناك حاجة ملحّة لتطوير قواعد بيانات أكثر تنوعاً وواقعية تشمل بيئات وإضاءة وهجمات مختلفة [128].
18. يعتمد نجاح أنظمة كشف التزوير على تكامل عدة عوامل تشمل جودة البيانات، قوة النماذج، وتعدد وسائل التحقق [129].

2.5 الأعمال المستقبلية المقترحة Proposed Future Works

1. من المتوقع أن يركز البحث على تحسين التعميم عبر المجالات (Domain Generalization) بحيث يمكن للنماذج التعامل مع هجمات غير معروفة وظروف بيئية مختلفة دون تدريب إضافي، وذلك استناداً إلى التحديات الحالية في التعميم في FAS [130].
2. هناك اتجاه قوي نحو تصميم خوارزميات مضادة للتزوير تعتمد على التعلم غير المشرف (Unsupervised) والتعلم شبه المشرف (Semi-Supervised) لتقليل الحاجة إلى بيانات موسومة وتحسين قابلية النموذج على التعميم [131].
3. سيستمر الباحثون في تطوير نماذج متعددة الوسائط (Multimodal) تدمج RGB وDepth وInfrared وحتى بيانات إضافية لتحسين الدقة والقدرة على كشف هجمات معقدة [132].
4. اقتراح إنشاء مجموعات بيانات جديدة ومتنوعة (More Comprehensive Datasets) تشمل أنماط جديدة من الهجمات مثل Deepfake وهجمات الإضاءة المنخفضة والتغيرات البيئية القصوى لمواجهة محدودية البيانات الحالية [133].
5. سيتجه البحث إلى تطوير شبكات خفيفة الوزن (Lightweight Networks) يمكن نشرها على الأجهزة المحمولة أو المدمجة دون فقدان الدقة، لتطبيق أنظمة كشف التزوير في الوقت الحقيقي [134].
6. هناك اهتمام متزايد بـ الأنظمة التكيفية في الوقت الحقيقي (Online Adaptive Systems) التي تتعلم وتتحسن تلقائياً مع وصول بيانات جديدة، لمواكبة الهجمات والبيئات المتغيرة باستمرار [135].
7. سيكون من الممكن أيضًا دمج تقنيات كشف موحدة للهجمات الرقمية والفيزيائية (Unified Digital & Physical Attack Detection) في إطار واحد، للتعامل مع Deepfake والهجمات الفيزيائية مثل الأقنعة والصور المطبوعة [134].

8. من المتوقع أن تتوسع الأبحاث في التعلم الفيدرالي (Federated Learning) لحماية خصوصية بيانات المستخدمين أثناء تدريب نماذج مضادة للتزوير من بيانات موزعة عبر أجهزة متعددة دون مشاركة البيانات الأصلية [135].
9. ينبغي تطوير معايير تقييم موحدة (Standard Evaluation Protocols) تشمل سيناريوهات متعددة وأنماط هجمات حديثة لتقييم أداء النماذج بشكل أكثر واقعية وشمولية [136].
10. أخيراً، فإن دمج تحليل الإشارات الحيوية (مثل rPPG) مع التعلم العميق يمكن أن يفتح آفاقاً جديدة لكشف التزوير اعتماداً على السمات الحيوية الدقيقة غير المستنسخة في عمليات التزييف الرقمية أو الفيزيائية [137,138].

من خلال هذه الجهود المستقبلية، يمكن تعزيز قدرات تقنيات الكشف عن تزوير بصمة الوجه، مما يفتح آفاقًا جديدة للتطبيقات العملية والبحثية في هذا المجال

REFERENCES

[1] Z. Yu et al., “Deep learning for face anti-spoofing: A survey,” IEEE Trans. Pattern Anal. Mach. Intell., 2022.

[2] Z. Ming et al., “A survey on anti-spoofing methods for facial recognition with RGB cameras of generic consumer devices,” Sensors, 2020.

[3] H. Xing et al., “Face anti-spoofing based on deep learning: A comprehensive survey,” Applied Sciences, vol. 15, 2025, Art. no. 6891.

[4] V. V. Chakole, “Review on methods of antispoofing in face recognition,” AIP Conf. Proc., 2024

[5] H. T. Mohammad et al., “Face spoofing detection using deep CNN,” Int. J. Adv. Comput. Sci. Appl., 2021.

[6] A. Kot et al., “Learning deep forest for face anti-spoofing: An alternative to the neural network against adversarial attacks,” Applied Sciences, 2024.

[7] W. D. Callister et al., Materials Science and Engineering: An Introduction, 10th ed. Wiley, 2020

[8] D. R. Askeland et al., The Science and Engineering of Materials, 8th ed. Cengage Learning, 2020.

[9] J. I. Goldstein et al., Scanning Electron Microscopy and X-ray Microanalysis, 5th ed. Springer, 2021.

[10] D. B. Williams et al., Transmission Electron Microscopy: ATextbook for Materials Science, 3rd ed. Springer, 2020.

[11] M. De Graef et al., Structure of Materials: An Introduction to Crystallography, Diffraction and Symmetry, 3rd ed. Cambridge University Press, 2022.

[12] C. S. S. R. Kumar (Ed.), Characterization Techniques for Nanomaterials. Springer, 2021.

[13] H. J. Bunge et al., “Advances in electron backscatter diffraction,” Ultramicroscopy, vol. 222, 2021, Art. no. 113210.

[14] S. Hofmann, “Auger- and X-ray photoelectron spectroscopy in materials science,” Surf. Interface Anal., vol. 52, no. 6, pp. 305–317, 2020.

[15] C. R. Brundle et al., Encyclopedia of Materials Characterization: Surfaces, Interfaces, Thin Films. Butterworth-Heinemann, 2021.

[16] B. D. Cullity et al., Elements of X-ray Diffraction, 4th ed. Pearson, 2022

[17] Y. Zhang et al., “Depth profiling techniques for material characterization: A review,” Mater. Charact., vol. 198, 2023, Art. no. 112684.

[18] ASTM International, ASTM E112 – Standard Test Methods for Determining Average Grain Size, 2020.

[19] E. O. Hall, “The deformation and ageing of mild steel,” Proc. Phys. Soc., 1951.

[20] N. J. Petch, “The cleavage strength of polycrystals,” J. Iron Steel Inst., 1953.

[21] ASM International, ASM Handbook, Volume 9: Metallography and Microstructures, 2004.

[22] ASTM International, Standard Test Methods for Porosity and Image Analysis in Materials, 2020.

[23] W. D. Callister et al., Materials Science and Engineering: An Introduction, 10th ed. Wiley, 2020

[24]R. Szeliski, Computer Vision: Algorithms and Applications. Springer, 2011

[25]R. Lange, “3D time-of-flight distance measurement with custom solid-state image sensors,” PhD dissertation, University of Siegen, 2000.

[26]A. Kolb et al., “Time-of-flight cameras in computer graphics,” IEEE Trans. Pattern Anal. Mach. Intell., 2010.

[27]M. Hansard et al., Springer Handbook of Computer Vision. Springer, 2012.

[28]R. Lange, “3D time-of-flight distance measurement with custom solid-state image sensors,” PhD dissertation, University of Siegen, 2000.

[29]G. Vosselman et al., Airborne and Terrestrial Laser Scanning. Whittles Publishing, 2010.

[30]J. Wang et al., “High-resolution 3D face scanning for biometric applications,” IEEE Trans. Instrum. Meas., vol. 65, no. 9, pp. 2025–2034, 2016

[31]S. K. Nayar et al., “Shape from focus,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 16, no. 8, pp. 824–831, 1994.

[32]M. Subbarao, “Parallel depth estimation from image focus,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 10, no. 2, pp. 137–154, 1988.

[33]X. Tao et al., “A theory of 3D imaging with large depth of field using stereo and focus,” Int. J. Comput. Vis., vol. 19, no. 3, pp. 237–258, 1995.

[34]C. Suárez et al., “Depth from focus using an active vision system,” Comput. Vis. Image Underst., vol. 62, no. 1, pp. 95–111, 1994.

[35]A. Pentland, “A new sense for depth of field,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 9, no. 4, pp. 523–531, 1987.

[36]Z. Boulkenafet et al., “OULU-NPU: A mobile face presentation attack database with real-world variations,” in Proc. IEEE FG, 2017.

[37]Z. Zhang et al., “A face antispoofing database with diverse attacks,” in Proc. ICB, 2012.

[38]I. Chingovska et al., “On the effectiveness of local binary patterns in face anti-spoofing,” in Proc. BIOSIG, 2012.

[39]ISO/IEC 30107-3:2017, Biometric Presentation Attack Detection – Part 3: Testing and Reporting.

[40]A. K. Jain et al., “An introduction to biometric recognition,” IEEE Trans. Circuits Syst. Video Technol., 2004.

[41]M. Turk et al., “Eigenfaces for recognition,” J. Cogn. Neurosci., 1991.

[42]T. Ahonen et al., “Face recognition with local binary patterns,” IEEE Trans. Pattern Anal. Mach. Intell., 2006.

[43]Y. Taigman et al., “DeepFace: Closing the gap to human-level performance in face verification,” in CVPR, 2014.

[44]F. Schroff et al., “FaceNet: A unified embedding for face recognition and clustering,” in CVPR, 2015

[45]M. Turk et al., “Eigenfaces for recognition,” J. Cogn. Neurosci., 1991.

[46]P. Belhumeur et al., “Eigenfaces vs. Fisherfaces: Recognition using class specific linear projection,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 19, no. 7, pp. 711–720, 1997.

[47]T. Ahonen et al., “Face description with local binary patterns: Application to face recognition,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 28, no. 12, pp. 2037–2041, 2006.

[48]Y. Taigman et al., “DeepFace: Closing the gap to human-level performance in face verification,” in CVPR, 2014

[49]Computer Vision and Image Understanding, “A survey on deep learning based face recognition,” Elsevier, 2019.

[50]F. Schroff et al., “FaceNet: A unified embedding for face recognition and clustering,” in CVPR, 2015, pp. 815–823.

[51]J. Deng et al., “ArcFace: Additive angular margin loss for deep face recognition,” in CVPR, 2019, pp. 4690–4699.

[52]J. Deng et al., “ArcFace: Additive angular margin loss for deep face recognition,” IEEE Trans. Pattern Anal. Mach. Intell., vol. 44, no. 9, pp. 4655–4669, 2022.

[53]Y. Srivastava et al., “A performance comparison of loss functions for deep face recognition,” arXiv preprint, 2019.

[54]A. Sumsion et al , “Surveying racial bias in facial recognition: Balancing datasets and algorithmic enhancements,” Electronics, vol. 13, no. 12, Art. 2317, 2024.

[55] I. Sarridis et al., (reference incomplete – needs full details) , “Towards Fair Face Verification: An In-depth Analysis of Demographic Biases,” arXiv, 2023.

[56] M. Wang et al., “Racial Faces in-the-Wild: Reducing Racial Bias by Information Maximization Adaptation Network,” arXiv, 2018.

[57] M. Gwilliam et al., “Rethinking Common Assumptions to Mitigate Racial Bias in Face Recognition Datasets,” arXiv, 2021.

[58] J. Coe et al., “Evaluating Impact of Race in Facial Recognition across Machine Learning and Deep Learning Algorithms,” Computers, vol. 10, no. 9, art. 113, 2021.

[59] J. Buolamwini et al., “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” Proc. Conf. Mach. Learn. Res., 2018.

[60] P. Terhörst et al., “Post-Comparison Mitigation of Demographic Bias in Face Recognition Using Fair Score Normalization,” arXiv preprint, 2020.

[61] B. F. Klare et al., “Pushing the Frontiers of Unconstrained Face Detection and Recognition: IARPA Janus Benchmark A,” Proc. CVPRW, 2015.

[62] I. D. Raji et al., “Actionable Auditing: Investigating the Impact of Publicly Naming Biased Performance Results of Commercial AI Products,” Proc. Conf. FAT, 2019.

[63] T. Wang et al., “Mitigating Bias in Face Recognition Using Domain-Balanced Training,” Proc. CVPRW, 2020.

[64] Z. Yu et al., “Face Anti-Spoofing Using Deep Learning: A Survey,” IEEE Trans. Inf. Forensics Security, vol. 16, pp. 1–19, 2021.

[65] I. Masi et al., “Deep Face Recognition: A Survey,” Proc. CVPRW, 2018.

[66] A. George et al., “Deep Pixel-wise Binary Supervision for Face Presentation Attack Detection,” Proc. ICB, 2019.

[67] S. Jia et al., “Multi-Scale Temporal Features for Face Anti-Spoofing,” Pattern Recognit. Lett., vol. 138, pp. 423–429, 2020.

[68] Y. Wang et al., “Domain Generalization for Face Anti-Spoofing,” IEEE Trans. Biometrics, Behavior, and Identity Sci., vol. 3, no. 4, pp. 1–12, 2021.

[69] T. Li et al., “Multimodal Face Anti-Spoofing Based on RGB and Depth Information,” IEEE Access, vol. 8, pp. 123–134, 2020.

[70] Z. Yu et al., “Searching Central Difference Convolutional Networks for Face Anti-Spoofing,” Proc. CVPR, 2020, pp. 5295–5305.

[71] W. Sun et al., “Face Anti-Spoofing Based on Generalized Deep Learning Framework,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 1–15, 2020.

[72] Y. Li et al., “Exposing DeepFake Videos by Detecting Face Warping Artifacts,” Proc. CVPR Workshops, 2019.

[73] T. Qin et al., “Learning Generalized Face Anti-Spoofing Models,” arXiv preprint, 2019.

[74] A. G. Howard et al., “MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications,” arXiv preprint, 2017.

[75] N. Erdogmus et al., “Spoofing Face Recognition with 3D Masks,” IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 1084–1097, 2014.

[76] A. K. Jain et al., Introduction to Biometrics, Springer, 2011.

[77] J. Yang et al., “Learn Convolutional Neural Network for Face Anti-Spoofing,” arXiv preprint, 2014.

[78] H. H. Nguyen et al., “Multi-task Learning for Detecting and Segmenting Manipulated Facial Images and Videos,” Proc. ICB, 2019.

[79] D. Gunning et al., “DARPA’s Explainable Artificial Intelligence (XAI) Program,” AI Mag., vol. 40, no. 2, pp. 44–58, 2019.

[80] Z. Zhang et al., “A Face Anti-Spoofing Database with Diverse Attacks,” Proc. ICB, 2012.

[81] A. Agarwal et al., “Face anti-spoofing using color texture analysis,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 10, pp. 2268–2278, 2016.

[82] L. Li et al., “Learn convolutional neural networks for face anti-spoofing,” arXiv, 2016.

[83] S. Zhang et al., “Face anti-spoofing via central difference convolutional networks,” in Proc. CVPR, 2020, pp. 5295–5305.

[84] H. Nguyen et al., “Multi-task learning for detecting and segmenting manipulated facial images,” in Proc. ICB, 2019.

[85] J. Buolamwini et al., “Gender shades: Intersectional accuracy disparities in commercial gender classification,” in Proc. FATML, 2018.

[86] T. Wang et al., “Domain balanced training for fair face recognition,” in Proc. CVPR Workshops, 2020.

[87] Z. Yu et al., “Face anti-spoofing survey: Algorithms, datasets challenges,” IEEE Trans. Inf. Forensics Security, vol. 16, pp. 1–19, 2021

[88] Masi et al., “Deep face recognition: A survey,” in Proc. CVPR Workshops, 2018.

[89] A. George et al., “Deep pixel-wise binary supervision for face presentation attack detection,” in Proc. ICB, 2019.

[90] S. Jia et al., “Multi-scale temporal features for face anti-spoofing,” Pattern Recognit. Lett., vol. 138, pp. 423–429, 2020.

[91] J. Wang et al., “Domain generalization for face anti-spoofing,” IEEE Trans. Biometrics, Behavior, and Identity Sci., vol. 3, no. 4, 2021

[92] T. Li et al., “Multimodal face anti-spoofing based on RGB and depth information,” IEE Access, vol. 8, pp. 123–134, 2020.

[93] Z. Yu et al., “Searching central difference convolutional networks for face anti-spoofing,” in Proc. CVPR, pp. 5295–5305, 2020.

[94]W. Sun et al., “Face anti-spoofing based on generalized deep learning framework,” IEEE Trans. Inf. Forensics Security, vol. 15, 2020.

[95] Y. Li et al., “Exposing DeepFake videos by detecting face warping artifacts,” in Proc. CVPR Workshops, 2019.

[96] T. Qin et al., “Learning generalized face anti-spoofing models,” arXiv, 2019.

[97] A. Howard et al., “MobileNets: Efficient convolutional neural networks for mobile vision applications,” arXiv, 2017.

[98] N. Erdogmus et al., “Spoofing face recognition with 3D masks,” IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 1084–1097, 2014.

[99] A. K. Jain et al., Introduction to Biometrics. Springer, 2011.

[100] J. Yang et al., “Learn convolutional neural network for face anti-spoofing,” arXiv, 2014.

[101] H. H. Nguyen et al., “Multi-task learning for detecting and segmenting manipulated facial images and videos,” in Proc. ICB, 2019.

[102] D. Gunning et al., “DARPA’s explainable artificial intelligence (XAI) program,” AI Magazine, vol. 40, no. 2, pp. 44–58, 2019.

[103] Z. Zhang et al., “A face anti-spoofing database with diverse attacks,” in Proc. ICB, 2012.

[104] A. Agarwal et al., “Face anti-spoofing using color texture analysis,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 10, pp. 2268–2278, 2016.

[105] L. Li et al., “Learn convolutional neural networks for face anti-spoofing,” arXiv, 2016.

[106] S. Zhang et al., “Face anti-spoofing via central difference convolutional networks,” in Proc. CVPR, 2020.

[107] H. Nguyen et al., “Multi-task learning for detecting and segmenting manipulated facial images,” in Proc. ICB, 2019.

[108] K. Patel et al., “Secure face authentication with 3D masks,” Pattern Recognit. Lett., vol. 120, pp. 1–9, 2019.

[109] X. Yang et al., “Face anti-spoofing with depth supervision,” IEEE Trans. Image Process., vol. 29, pp. 3505–3518, 2020.

[110] M. Liu et al., “Deep learning-based face anti-spoofing: A survey,” IEEE Access, vol. 8, pp. 163–181, 2020.

[111] Y. Liu et al., “Racial Faces in-the-Wild: Reducing Racial Bias in Face Recognition,” Proc. ECCV, 2018.

[112] J. Buolamwini et al., “Gender Shades: Intersectional Accuracy Disparities in Commercial Gender Classification,” Proc. FATML, 2018.

[113] T. Wang et al., “Domain Balanced Training for Fair Face Recognition,” Proc. CVPRW, 2020.

[114] Z. Yu et al., “Face Anti-Spoofing Survey: Algorithms, Datasets and Challenges,” IEEE Trans. Inf. Forensics Security, vol. 16, pp. 1–19, 2021.

[115] I. Masi et al., “Deep Face Recognition: A Survey,” Proc. CVPRW, 2018.

[116] A. George et al., “Deep Pixel-wise Binary Supervision for Face Presentation Attack Detection,” Proc. ICB, 2019.

[117] S. Jia et al., “Multi-Scale Temporal Features for Face Anti-Spoofing,” Pattern Recognit. Lett., vol. 138, pp. 423–429, 2020.

[118] Y. Wang et al., “Domain Generalization for Face Anti-Spoofing,” IEEE Trans. Biometrics, Behavior, and Identity Sci., vol. 3, no. 4, pp. 1–12, 2021.

[119] T. Li et al., “Multimodal Face Anti-Spoofing Based on RGB and Depth Information,” IEEE Access, vol. 8, pp. 123–134, 2020.

[120] Z. Yu et al., “Searching Central Difference Convolutional Networks for Face Anti-Spoofing,” Proc. CVPR, 2020, pp. 5295–5305.

[121] W. Sun et al., “Face Anti-Spoofing Based on Generalized Deep Learning Framework,” IEEE Trans. Inf. Forensics Security, vol. 15, pp. 1–15, 2020.

[122] Y. Li et al., “Exposing DeepFake Videos by Detecting Face Warping Artifacts,” Proc. CVPRW, 2019.

[123] T. Qin et al., “Learning Generalized Face Anti-Spoofing Models,” arXiv preprint, 2019.

[124] A. Howard et al., “MobileNets: Efficient Convolutional Neural Networks for Mobile Vision Applications,” arXiv preprint, 2017.

[125] N. Erdogmus et al., “Spoofing Face Recognition with 3D Masks,” IEEE Trans. Inf. Forensics Security, vol. 9, no. 7, pp. 1084–1097, 2014.

[126] A. Jain et al., Introduction to Biometrics, Springer, 2011.

[127] J. Yang et al., “Learn Convolutional Neural Network for Face Anti-Spoofing,” arXiv preprint, 2014.

[128] H. Nguyen et al., “Multi-task Learning for Detecting and Segmenting Manipulated Facial Images and Videos,” Proc. ICB, 2019.

[129] D. Gunning et al., “DARPA’s Explainable Artificial Intelligence (XAI) Program,” AI Mag., vol. 40, no. 2, pp. 44–58, 2019.

[130] Z. Zhang et al., “A Face Anti-Spoofing Database with Diverse Attacks,” Proc. ICB, 2012.

[131] A. Agarwal et al., “Face Anti-Spoofing Using Color Texture Analysis,” IEEE Trans. Inf. Forensics Security, vol. 11, no. 10, pp. 2268–2278, 2016.

[132] L. Li et al., “Learn Convolutional Neural Networks for Face Anti-Spoofing,” arXiv preprint, 2016.

[133] S. Zhang et al., “Face Anti-Spoofing via Central Difference Convolutional Networks,” Proc. CVPR, 2020, pp. 5295–5305.

[134] H. Nguyen et al., “Multi-task Learning for Detecting and Segmenting Manipulated Facial Images,” Proc. ICB, 2019.

[135] K. Patel et al., “Secure Face Authentication with 3D Masks,” Pattern Recognit. Lett., vol. 120, pp. 1–9, 2019.

[136] X. Yang et al., “Face Anti-Spoofing with Depth Supervision,” IEEE Trans. Image Process., vol. 29, pp. 3505–3518, 2020.

[137] M. Liu et al., “Deep Learning-Based Face Anti-Spoofing: A Survey,” IEEE Access, vol. 8, pp. 163–181, 2020.

[138] Y. Liu et al., “Racial Faces in-the-Wild: Reducing Racial Bias in Face Recognition,” Proc. ECCV, 2018.