المجلة العلمية المُحكمة للأكاديمية العربية الدولية
The Scientific Journal of the International Arab Academy
رقم شهادة عضوية اتحاد الجامعات الدولي (IUU): 1102202600217 ـ رقم شهادة معامل التأثير العربي: (287)
ISSN (ONLINE): 1858 - 8441 - ISSN (PRINT): 1858 - 845X

(3)

# اكتشاف الوجه الحقيقي بإستخدام تقنية التعلم العميق علي الموبايل

د. ابراهيم محمد أحمد علي
جامعة كرري كلية الحاسوب وتقانة المعلومات
البريد الالكتروني
Ibrahim1630@gmail.com

المجلة العلمية المُحكمة للأكاديمية العربية الدولية
The Scientific Journal of the International Arab Academy
رقم شهادة عضوية اتحاد الجامعات الدولي (IUU): 1102202600217 ـ رقم شهادة معامل التأثير العربي: (287)
ISSN (ONLINE): 1858 - 8441 - ISSN (PRINT): 1858 - 845X

**المستخلص**

**يشهد مجال الذكاء الاصطناعي تطورًا متسارعًا ينعكس في التطبيقات المتقدمة التي تُحدث تحولًا في مختلف القطاعات. تهدف هذه الورقة إلى عرض نظام ذكي تم تطويره باستخدام لغة البرمجة Python، ويعتمد على تقنيات التعلم العميق لمعالجة البيانات وتحليلها لإكتشاف الوجه الحقيقي. يتميز النظام بسهولة الاستخدام، وقد تم توظيفه في بيئات متعددة مثل أنظمة كشف الاحتيال الإلكتروني وقد اظهرت النتائج النجاح في تصنيف الصور بدقه عاليه تقدر بـ 98.56 %، مما يسهم في تعزيز مستويات الأمان وتقليل السلوكيات المشبوهة. كما يمكن تطبيقه في المؤسسات المالية والمستودعات والمتاجر الذكية، ليكون أداة فعالة في دعم اتخاذ القرار ومواجهة التهديدات الرقمية.**

**الكلمات المفتاحيه: الذكاء الاصطناعي، التعلم العميق، معالجة البيانات،كشف الاحتيال الإلكتروني، الأمن السيبراني، الأنظمة الذكية، اكتشاف الوجه الحقيقي.**

## Abstract

Technologies are advancing rapidly، particularly in the field of artificial intelligence. In this research، we present a system developed using Python that applies deep learning techniques to enhance data protection against spoofing attacks. The proposed anti-spoofing system identifies only live faces of users، thereby preventing unauthorized access. This approach significantly improves security levels and reduces risks of data and information theft. Further more، the system can be applied in sensitive environments such as banks and warehouses، where facial recognition ensures secure access and protection against spoofing attempts.

**Keywords:** Artificial intelligence، deep learning، data processing، online fraud detection، cyber security، intelligent systems، real-life facial recognition

## المقدمة:

نتيجة لتكرار عمليات القرصنة وتطوير الهاكرز «أساليبهم في الإحتيال ، بدأت الكثير من الدول وكبري شركات التكنولوجيا في البحث عن وسائل أنجع لحفظ أمن معلوماتهم ومن هنا كانت الهجرة الجماعية نحو أنظمة الأمن الحيوي» او مايطلق عليه أيضاً القياسات الحيوية [1].

فأن القياسات الحيوية هي تقنية لتحديد هوية الشخص أو التحقق منه عن طريق قياس أو تحليل سمات جسمه ، يمكن تصنيف هذه السمات بشكل أكبر الي سمات جسدية مثل : بصمة الأصبع والوجبه وشبكية العين والقزحية وما الي ذلك ، والسمات السلوكية مثل الصوت ووالتوقيع والمشي وما الي ذلك ، وتسمي هذة السمات أيضاً بطرق تقنيات تحديد الهوية أو الخصائص تستخدم أنظمة القياسات الحيوية حالياً في العديد من التطبيقات المختلفة تعد مراقبة الحدود والتسهيلات العسكرية والوصول عبر الهاتف المحمول الي الحسابات الشخصية او العمليات المصرفية من

المجلة العلمية المُحكمة للأكاديمية العربية الدولية
The Scientific Journal of the International Arab Academy
رقم شهادة عضوية اتحاد الجامعات الدولي (IUU): 1102202600217 ـ رقم شهادة معامل التأثير العربي: (287)
ISSN (ONLINE): 1858 - 8441 - ISSN (PRINT): 1858 - 845X

بعض التطبيقات التي تتطلب مستويات عالية من الموثوقية والمتانة يكاد لا يمر أسبوع إلا وتتعرض إحدي الشركات لإختراق بياناتها مسببة بذلك سرقة معلومات عن الآلاف من روادها او مستخدمي منتجاتها ، ناهيك عن الخسائر المادية الناتجة عن ذلك الأختراق [1].

القياسات الحيوية ضرورية لمجموعة واسعة من التقنيات، ومع ذلك فإن إحدى العقبات الرئيسية التي تواجه أنظمة التعرف على القياسات الحيوية هي الهوية المزورة والذي يشار اليه من الناحية المفاهيمية على انه هجوم انتحال [2].

بشكل عام يمكن اعتبار نوعين من الهجمات: هجمات غير مباشرة والهجمات المباشرة يتم تنفيذ الهجمات غير المباشرة داخل النظام ويتطفل عليها المتسللون او الدخلاء على سبيل المثال: عن طريق العبث بمستخرج الميزة (أي المطابق) او عن طريق اجراء تعديلات على قاعدة بيانات القالب [2].

يمكن منع الهجمات غيره المباشرة من خلال تدابير مختلفة بما في ذلك على سبيل المثال برامج مكافحات الفيروسات، جدران الحماية والتشفير وكشف التسلل. من ناحية أخرى يتم تنفيذ هجمات مباشره على جهاز الاستشعار خارج الحدود الرقمية للنظام وبالتالي لا يمكن استخدام أي آليات للحماية الرقمية لتوقع ذلك [2].

## بصمة الوجه

التعرف على الوجوه هو نهج حيوي مستخدم على نطاق واسع، تطورت تقنية التعرف على الوجوه بسرعة في السنوات الأخيرة وهو أكثر مباشرة وسهولة في الاستخدام وملاءمة مقارنة بالطرق الأخرى [3].

الهدف الرئيسي هو توفير ملف مسار التطوير المستقبلي لنهج الكشف عن حيوية الوجه الجديد والأكثر امانا لدى عامة الناس حاجة ماسه لاتخاذ تدابير امنية ضد الهجمات الخادع، القياسات الحيوية هي الجزء الأسرع نمواً في صناعة الامن هذه. بعض التقنيات المألوفة للتعرف على الوجه، التعرف على بصمة الأصابع، التحقق من خط اليد الماسح الضوئي لشبكية العين وقزحية العين. من بين هذه التقنيات، التي تطورت بسرعة في السنوات الأخيرة، أصبحت تقنية التعرف على الوجوه أكثر مباشره، وسهله الاستخدام، ومريحة مقارنه بالطرق الأخرى [1].

ونظراً لإستخدام التعرف علي الوجه بشكل متزايد للتحكم في الوصول والمصادقة ، وحراسة المعلومات الحساسة ، لذلك تم تطبيقه على أنظمة الأمان المختلفة ولكن بشكل عام، لا تستطيع خوارزميات التعرف على الوجوه التمييز بين الوجه " الحي " والوجه " غير الحي "وهي مشكلة امنية رئيسية، انها طريقة سهلة لخداع أنظمة التعرف على الوجوه عن طريق الصور مثل الصور الشخصية [4]. من اجل الحماية من مثل هذا الانتحال، نحتاج إلي نظام آمن بإستخدام القياسات الحيوية هي تقنية لتحديد هوية الفرد على أساس مادي او السمات السلوكية للشخص [5].

يتزايد الدافع لمهاجمة مثل هذة الأنظمة ويمكن مهاجمة انظمة التعرف علي الوجوه بإستخدام الصور المطبوعة أو الأقنعة أو شاشات الفيديو في القياسات الحيوية ويعد إكتشاف الحياة Liveness Detection هو قدرة الكمبيوتر علي تحديد ما اذاكان يتفاعل مع كائن بشري موجود جسدياً وليس قطعة أثرية ساخرة أو فيديو . [6]. فأن إكتشاف الحياة Liveness Detection هو الذكاء الإصطناعي الذي يحدد ما إذا كان الكبيوتر يتفاعل مع إنسان حي [2] .

## التعلم العميق (Deep Learning)

هو مجال بحث جديد يتناول إيجاد نظريات وخوارزميات تتيح للآلة أن تتعلم بنفسها عن طريق محاكاة الخلايا العصبية في جسم الإنسان وأحد فروع العلوم التي تتناول علوم الذكاء الاصطناعي[٧].

المجلة العلمية المُحكمة للأكاديمية العربية الدولية
The Scientific Journal of the International Arab Academy
رقم شهادة عضوية اتحاد الجامعات الدولي (IUU): 1102202600217 ـ رقم شهادة معامل التأثير العربي: (287)
ISSN (ONLINE): 1858 - 8441 - ISSN (PRINT): 1858 - 845X

يعد فرع من فروع علوم التعلم الآلي وأثبتت الاكتشافات في هذا المجال تقدما كبيرا وسريعا وفعالية في العديد المجالات منها التعرف على الوجه التعرف على الكلام الرؤية الحاسوبية ومعالجة اللغات الطبيعية [8].

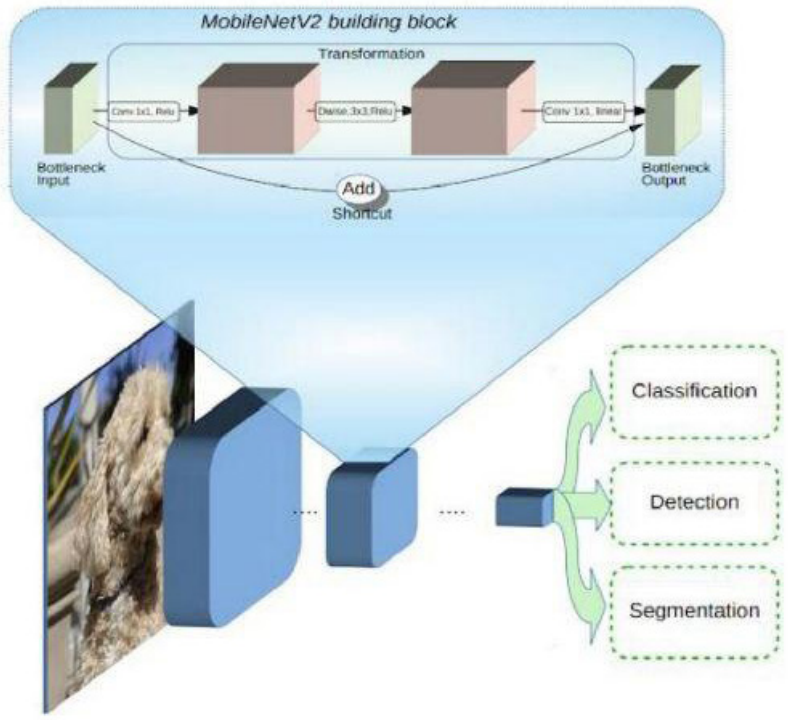
تتعلم الآلة من البيانات الضخمة باستخدام تصميمات مختلفة لشبكات التعلم العميق منها: الشبكات المتكررة (RNN) المستخدمة بكثرة مع النصوص والبيانات المستمرة والشبكة عصبونية التفافية (CNN) التي تستمد التهامها من العمليات البيولوجية في الفص البصري وغيرها من التصميمات [8].

## الشبكة العصبية الالتفافية (Convolutional Neural Network – CNN)

الشبكة العصبية الالتفافية هي شبكة عصبية اصطناعية فعالة بشكل خاص وتقدم بنية فريدة من نوعها. يتم تنظيم الطبقات في ثلاثة أبعاد: العرض والارتفاع والعمق. الخلايا العصبية في طبقة واحدة لا تتصل بجميع الخلايا العصبية في الطبقة التالية ولكن فقط إلى منطقة صغيرة من الخلايا العصبية للطبقة. يتم تقليل الإخراج النهائي إلى متجه واحد من درجات الاحتمال منظم على طول بعد العمق [9].

## خوارزمية MobileNetV2

يعد MobileNetV2 من أحدث التقنيات للتعرف البصري على الأجهزة المحمولة بما في ذلك التصنيف واكتشاف الكائنات والتجزئة الدلالية. تم إصدار MobileNetV2 كجزء من مكتبة تصنيف الصور TensorFlow-Slim،[10]، يعتمد MobileNetV2 على الأفكار من MobileNetV1 باستخدام التفاف عميق قابل للفصل ككتل بناء فعالة [11]، الشكل (1) يعطي نظره عامه علي هندسه موبايل نت2.

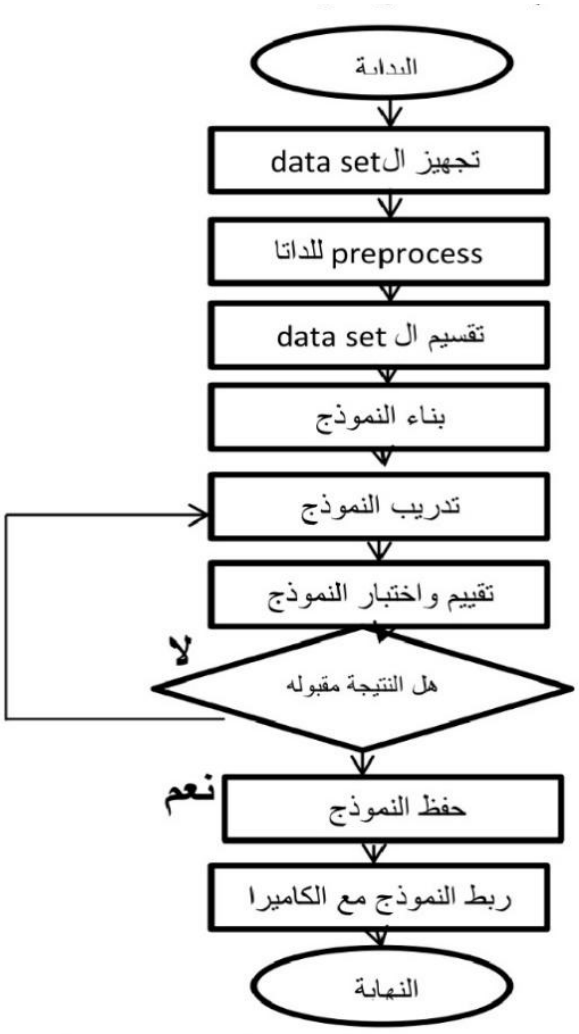



**الشكل (1) هيكل عمل الـ MobileNetV2**

المجلة العلمية المُحكمة للأكاديمية العربية الدولية
The Scientific Journal of the International Arab Academy
رقم شهادة عضوية اتحاد الجامعات الدولي (IUU): 1102202600217 ـ رقم شهادة معامل التأثير العربي: (287)
ISSN (ONLINE): 1858 - 8441 - ISSN (PRINT): 1858 - 845X

## منهجية البحث

تم اتباع المنهج التحليلي لتحليل حالة المستخدمين ومقارنتها كل مرة للتأكد من تمييز الوجه الحقيقي من الوجه المزيف.كما يتم استخدام (نموذج أو خوارزمية) MobileNetV2 من خلال تسعه خطوات وهي) تثبيت بيئة العمل، تجهيز البيانات،استيراد المكاتب python ، عمل preprocess للبيانات، تقسيم data set الى train و test ،بناء النموذج ،تدريب الداتا على الشبكة ، تقييم النموذج بعد التدريب والاختبار ،ربط النموذج مع كاميرا الجهاز) كما موضح بالشكل (2) .




**الشكل (2) مخطط تدفق النظام**

**الخطوة الأولى:** تثبيت بيئة العمل:

– قمنا بتثبيت anaconda وتلقائياً يتم تثبيت python ضمنها وإنستخدم Spyder لكتابة الكود البرمجي.

**الخطوة الثانية:** تجهيز البيانات: بتحميل الـ Data set و رفع البيانات إلى Google Drive وتحميل Google Colab على Google Drive.

**الخطوة الثالثة:** استيراد المكتبات على Google Colab:

قمنا باستيراد مكتبات TensorFlow، keras ، matplotlib.pyplot ، imutils numpy

المجلة العلمية المُحكمة للأكاديمية العربية الدولية
The Scientific Journal of the International Arab Academy
رقم شهادة عضوية اتحاد الجامعات الدولي (IUU): 1102202600217 ـ رقم شهادة معامل التأثير العربي: (287)
ISSN (ONLINE): 1858 - 8441 - ISSN (PRINT): 1858 - 845X

**الخطوة الرابعة:** عمل Preprocess للبيانات.

**الخطوة الخامسة:** تقسيم الـ Data Set إلى Train و Test

تم تقسيم الداتا عن طريق النسبة (80 % – 20 %) حيث Train = 80 % و Test = 20 %.

**الخطوة السادسة:** بناء النموذج:

– بعد تجهيز الداتا قمنا باستدعاء النموذج MobileNetV2 لتطبيقه على الداتا

**الخطوة السابعة:** تدريب للداتا على الشبكة:

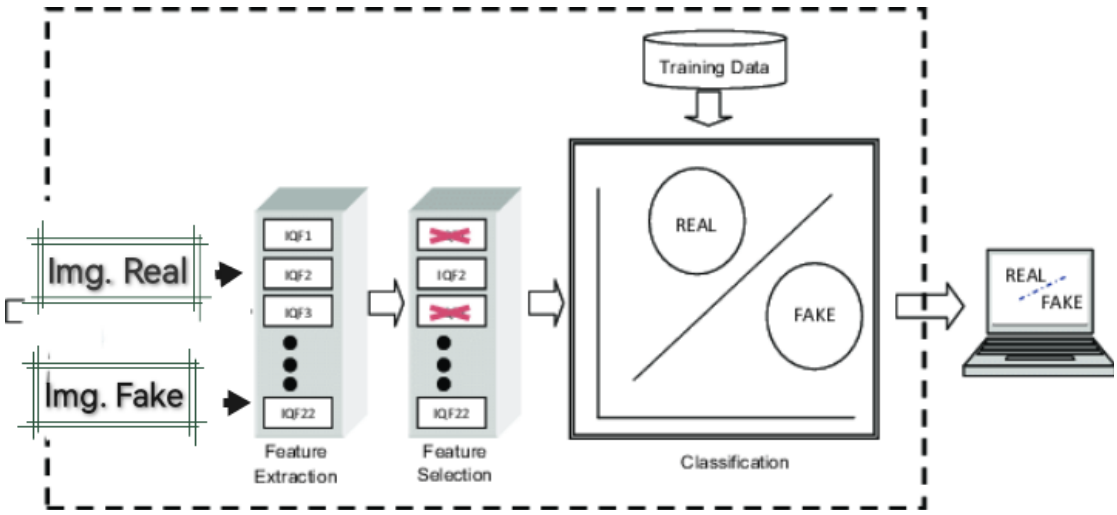
–قمنا بعمل imageDataGenerator لزيادة عدد الصور وذلك عن طريق(قص ، تدوير ، تكبير ، دوران…)

– لا نقوم بإعطاء الداتا مرة واحدة للتدريب، وإنما نقوم بتقسيمها حتى لا تحصل Overfitting.

**الخطوة الثامنة :** تقييم النموذج بعد التدريب والاختبار

عن طريق الدالة matplotlib.pyplot وهي خاصة برسم المنحنيات والرسم البياني في التقييم.

**الخطوة التاسعة:** ربط النموذج مع كاميرا الجهاز والشكل(3) التالي يوضح خلاصة عمل النظام

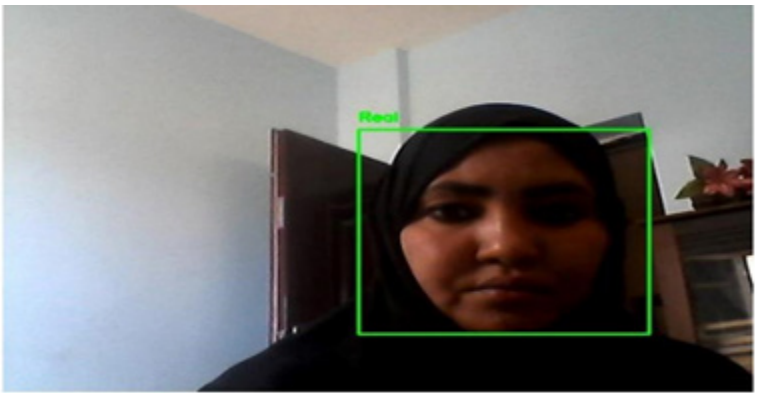



**الشكل (3) هيكل عمل النظام**

## التطبيق

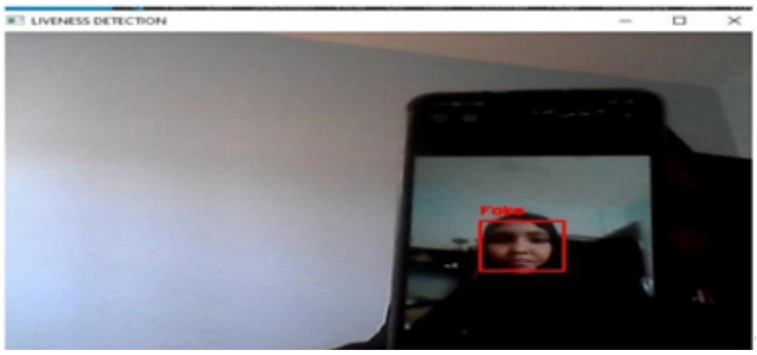
تم القيام بهذا العمل عن طريق جهاز لديه 2 قيقا بايت كرت شاشة خارجي (Radeon) من الجيل السابع ورام 8 قيقا بايت. تم العمل على منصة Google Colab حيث تعطيك GPU و RAM إضافتين مما حسن من النتائج بشكل كبير.

المجلة العلمية المُحكمة للأكاديمية العربية الدولية
The Scientific Journal of the International Arab Academy
رقم شهادة عضوية اتحاد الجامعات الدولي (IUU): 1102202600217 ـ رقم شهادة معامل التأثير العربي: (287)
ISSN (ONLINE): 1858 - 8441 - ISSN (PRINT): 1858 - 845X

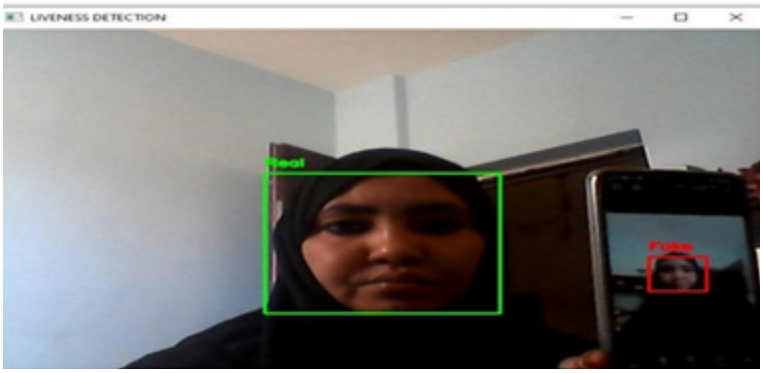



**الشكل (4) صوره حقيقية (real)**

الشكل(4) يوضح ان الصورة حقيقية بينما الشكل(5) يوضح بان الصورة غيرة مباشره والشكل(6) بها صوريتين واحدة مباشرة والثانيه صورة للاصل




**الشكل (5) صوره مزيفة (fake)**




**الشكل (6) صوره حقيقية (real) وصوره مزيفة (fake)**

## النتائج

أظهرت النتائج أن الموديل نجح في تصنيف الصور بدقة عالية بلغت 98.56%، مع تأكيد أن جودة الصور وحجم بيانات التدريب يلعبان دوراً محورياً في تحسين الأداء، حيث كلما زادت البيانات التدريبية ارتفعت دقة التصنيف، وكلما تحسنت جودة الصور انعكس ذلك إيجاباً على النتائج. كما تبين أن عملية استخراج الخصائص تحتاج إلى موازنة بين سهولة الاستخراج وجودة الصور، وأن الموديل قد يتطلب إعادة التدريب أكثر من مرة للوصول إلى مستوى تصنيف متقدم. إضافة إلى ذلك، تم التحقق من حيوية الشخص بدقة عالية جداً، ولم يُلاحظ أي Overfitting، إذ أظهرت التجارب المتكررة ارتفاعاً في الـ Validation accuracy وانخفاضاً في الـ Validation loss، مما يعكس كفاءة الموديل واستقراره.

## المراجع

[1] Chingovska، I.، A. Anjos، and S. Marcel. *On the effectiveness of local binary patterns in face anti-spoofing*. In 2012 BIOSIG-proceedings of the international conference of biometrics special interest group (BIOSIG). 2012. IEEE.

[2] Hernandez-Ortega، J.، et al.، *Introduction to presentation attack detection in face biometrics and recent advances*. 2023: p. 203-230.

[3] de Freitas Pereira، T. et al.، *Face liveness detection using dynamic texture*. 2014. 2014(1): p. 2.

[4] Tan، X.، et al.، *Face Liveness Detection from a Single Image with Sparse Low Rank Bilinear Discriminative Model*. 2010. 6316: p. 504-517.

[5] Jain، A.K. and S.Z. Li، *Handbook of face recognition*. Vol. 1. 2011: Springer.

[6] Uludag، U. and A.K. Jain. *Attacks on biometric systems: a case study in fingerprints*. In Security، steganography، and watermarking of multimedia contents VI. 2004. SPIE.

[7] Fumera، G.، et al.، *Multimodal anti-spoofing in biometric recognition systems*. 2014: p. 165-184.

[8] Bacciu، D.، et al.، *A gentle introduction to deep learning for graphs*. 2020. 1: 29p. 203-221.

[9] Xie، X.-Z.، et al.، *DG-CNN: Introducing Margin Information into Convolutional Neural Networks for Breast Cancer Diagnosis in Ultrasound Images*. 2022. 37(2): p. 277-294.

[10] Dürr، O.، B. Sick، and E. Murina، *Probabilistic deep learning : With python، keras and tensorflow probability*. 2020: Manning Publications.

[11] Zhang، Z.، et al. *A face antispoofing database with diverse attacks*. in *2012 5th IAPR international conference on Biometrics (ICB)*. 2012. IEEE.