Journal of Technology Research (JTR)
Volume 3, Issue 2, (2025), pp 092-102, ISSN 3005-639X

An Efficient Hybrid MobileNetV3–LightGBM Framework for Image-Based Malware Detection

Ali A. Elrowayati [*1], Ayman E. Abufanas [2], ObaidAllah H. Albedy[1]

[1]Elctronic Engineering Department, The College of Industrial Technology, Misurata, Libya.

[2]Computer Technologies Department, The High Institute of Science and Technology, Misurata, Libya.

*Corresponding author email: elrowayati@yahoo.com.

Received: 29-10-2025 | Accepted: 05-12-2025 | Available online: 15-12-2025 | DOI:10.26629/jtr.2025.11

ABSTRACT

Traditional signature-based malware detection techniques have become inadequate in addressing the complexity of modern cybersecurity threats. To overcome these limitations, this paper presents an intelligent malware classification framework that leverages computer vision and deep learning. The Malimg dataset, consisting of grayscale images representing diverse malware families, was utilized to facilitate structural and behavioural feature extraction. The hybrid MobileNetV3–LightGBM model proposed in this paper combines the lightweight MobileNetV3 architecture for efficient deep feature representation with the Light Gradient Boosting Machine (LightGBM) for robust and accurate classification. Experimental results demonstrate that the proposed model outperforms conventional deep learning approaches such as CNN and CNN–SVM, achieving an accuracy of 97.6%, with precision, recall, and F1-score averaging 98%. These findings confirm that integrating lightweight convolutional networks with gradient-boosted decision techniques significantly enhances malware detection performance and generalization. The proposed framework provides a scalable and effective solution for real-time malware analysis and establishes a foundation for future research on adaptive and explainable AI-driven cybersecurity systems.

Keywords: Convolutional neural networks, Deep learning, ImageNet, LightGBM, MobileNetV3.

نموذج هجين للكشف عن البرمجيات الخبيثة باستخدام الصور بالاعتماد على التعلم العميق وتقنيات التعزيز التدريجي

علي عبدالحفيظ الروياتي[1]، أيمن السنوسي أبوفناس[2]، عبيدالله حسن البيدي[1]

[1]قسم هندسة الحاسوب، كلية التقنية الصناعية، مصراتة، ليبيا.

[2]قسم تقنيات الحاسوب، المعهد العالي للعلوم والتقنية، مصراتة، ليبيا

ملخـــــص البحـــــث

شهد مجال أمن المعلومات تطورًا متسارعًا في أساليب الهجوم الإلكتروني، مما يجعل أنظمة الكشف التقليدية المعتمدة على التواقيع الثابتة غير كافية للتعامل مع التهديدات الحديثة. تهدف هذه الورقة إلى تطوير إطار هجين فعّال للكشف عن البرمجيات الخبيثة باستخدام الصور بالاعتماد على تقنيات التعلّم العميق والتعزيز التدريجي، من خلال دمج قوة استخلاص

الميزات البصرية العميقة مع كفاءة نماذج التصنيف الحديثة. تم استخدام قاعدة بيانات Malimg التي تحتوي على صور رمادية تمثل عينات متنوعة من البرمجيات الخبيثة مصنّفة إلى فئات متعددة، وذلك لتدريب النموذج المقترح وتقييم أدائه. اعتمدت الورقة على معمارية MobileNetV3 لاستخلاص الميزات البصرية المميّزة لكل فئة، نظرًا لكفاءتها العالية وخفة وزنها، بينما استُخدمت خوارزمية Light Gradient Boosting Machine (LightGBM) كطبقة تصنيف نهائية لتعزيز الدقة وتقليل فرط التعلّم. أظهرت النتائج أن النموذج الهجين MobileNetV3–LightGBM حقق أداءً متميزًا مقارنةً بالنماذج التقليدية مثل CNN وCNN–SVM، بدقة تصل الى ما يقارب 98% ومتوسط Precision وRecall وF1–score بلغ 98%. تبرز هذه النتائج فعالية الدمج بين تقنيات التعلّم العميق وخوارزميات التعزيز التدريجي في بناء أنظمة ذكية ودقيقة للكشف عن البرمجيات الخبيثة، مما يمهّد لتطبيقات عملية في مجال الأمن السيبراني في الزمن الحقيقي.

الكلمات الدالة: الشبكات العصبية الالتفافية، التعلم العميق، الكشف عن البرمجيات الخبيثة، الرؤية الحاسوبية، التعلم الالي.

1. المقدمـة

يمثل التطور السريع وانتشار البرمجيات الخبيثة (Malware) تهديدًا متزايدًا ومستمرًا للأفراد والمؤسسات والبنية التحتية الحيوية في جميع أنحاء العالم. إذ يمكن أن تؤدي هجمات البرمجيات الخبيثة إلى عواقب وخيمة تشمل اختراقات البيانات، والخسائر المالية، وتعطيل الأنظمة التشغيلية، وفقدان المعلومات الحساسة [1].

تعتمد أساليب الكشف التقليدية عادةً على التوقيعات (Signatures)، حيث يتم مطابقة الأنماط المعروفة داخل الملفات التنفيذية مع قاعدة بيانات تحتوي على تواقيع تهديدات سابقة. وعلى الرغم من فعالية هذه الأساليب في التعرف على التهديدات المعروفة، فإنها تفشل غالبًا في اكتشاف البرمجيات الخبيثة الجديدة أو المتعددة الأشكال (Polymorphic Malware) التي تغيّر بنيتها البرمجية باستمرار لتفادي الكشف[2]. ونتيجة لذلك، تصبح آليات الدفاع ذات طبيعة تفاعلية بدلاً من أن تكون استباقية.

لمعالجة قيود الأساليب التقليدية وتعزيز القدرة على اكتشاف البرمجيات الخبيثة غير المعروفة مسبقًا، اتجه الباحثون نحو التحليل المستند إلى الصور (Image–based Analysis)، الذي يقوم بتحويل الملفات الثنائية إلى تمثيلات بصرية (Gray–scale Images). يتيح هذا النهج تطبيق تقنيات رؤية الحاسوب (Computer Vision) وخوارزميات التعلم العميق (Deep Learning) على مشكلة تصنيف البرمجيات الخبيثة [3]. ومن خلال معاملة البرامج الخبيثة كصور رقمية، يمكن الاستفادة من قدرات الشبكات العصبية الالتفافية (CNNs) في تعلم الأنماط والخصائص المميزة لعائلات مختلفة من البرمجيات الخبيثة بصورة تلقائية، دون الحاجة إلى دوال مساندة لاستخلاص الميزات كما في التعلم الالي (Machine Learning)[4].

ورغم التقدم الملحوظ في هذا الاتجاه، ما زال تطوير نماذج تصنيف دقيقة وعالية الكفاءة يمثل تحديًا. إذ يتطلب بناء نموذج CNN فعال من الصفر كمية ضخمة من البيانات المصنفة وموارد حسابية كبيرة [5]. كما أن تحقيق أداء مستقر على مجموعات بيانات متعددة الفئات—خاصة تلك التي تحتوي على عينات محدودة لكل فئة—يستلزم نموذجًا يتمتع بقدرات قوية على استخلاص الميزات والتعميم [6].

استنادًا إلى ذلك، تهدف هذه الورقة إلى اقتراح وتقييم نموذج هجين جديد لتصنيف صور البرمجيات الخبيثة يجمع بين قوة التعلم الانتقالي (Transfer Learning) لاستخلاص الميزات وفعالية خوارزميات تعزيز التدرج (Gradient Boosting) في التصنيف.

يعتمد النموذج المقترح على استخدام MobileNetV3، وهي بنية خفيفة الوزن ومتقدمة من نماذج الشبكات العصبية الالتفافية، كمستخلص ميزات أساسي. وتُستخدم الميزات المستخرجة بعد ذلك كمدخلات لمُصنّف LightGBM، وهي خوارزمية تعلم آلي تعتمد على Gradient Boosting Decision Trees (GBDT) وتتميز بسرعة التنفيذ وكفاءتها العالية في التعامل مع البيانات عالية الأبعاد.

تتمثل المساهمات العلمية الرئيسة لهذا البحث فيما يلي:

- اقتراح نموذج هجين جديد (MobileNetV3 + LightGBM) يجمع بين التعلم الانتقالي واستخلاص الميزات والتصنيف المعزز، مما يحسن دقة تصنيف صور البرمجيات الخبيثة وكفاءتها الحسابية.
- تقييم شامل لأداء النموذج المقترح على مجموعة بيانات Malimg Dataset، مع إبراز قدرته على التمييز بين عائلات البرمجيات الخبيثة بدقة عالية.
- تحليل مقارن يوضح تفوق النموذج المقترح على النماذج التقليدية القائمة على CNN فقط، سواء من حيث الدقة أو الكفاءة الحسابية.

قسمت أجزاء الورقة على النحو التالي: يستعرض القسم الثاني الأعمال والدراسات ذات الصلة. فيما يتناول القسم الثالث المنهجية المقترحة، بما في ذلك مجموعة البيانات وعمليات ما قبل المعالجة واستخلاص الميزات باستخدام MobileNetV3، وآلية التصنيف بخوارزمية LightGBM. يقدم القسم الرابع النتائج التجريبية ويناقشها. وأخيرًا، يتناول القسم 5 الاستنتاجات والآفاق المستقبلية للبحث.

2. الدراسات السابقة

أدى التطور المتسارع في أساليب الهجمات الإلكترونية إلى دفع الباحثين نحو تبني تقنيات متقدمة قائمة على رؤية الحاسوب والتعلم العميق للكشف عن البرمجيات الخبيثة.

ونظرًا لندرة الدراسات العربية المتخصصة في هذا المجال، فقد تم استعراض الأدبيات الأجنبية الأحدث والأكثر تأثيرًا ذات الصلة.

يُعدّ عمل Nataraj وآخرون (2011) من أوائل الدراسات التي اقترحت تحويل البرمجيات الخبيثة إلى صور رقمية بهدف تحليلها بصريًا. استخدم الباحثون مجموعة بيانات مكونة من 9339 عينة موزعة على 25 عائلة مختلفة، واستخدموا واصف GIST لاستخراج السمات من الصور قبل تصنيفها بخوارزمية k–NN، محققين دقة بلغت 98%. ومع ذلك، واجه النهج صعوبة في الكفاءة الحسابية نظرًا لتعقيد عمليات استخلاص الميزات [4].

وفي عام 2018، قدّم Quan Le وآخرون نموذجًا للتعلم العميق يعتمد على الشبكات العصبية الالتفافية (CNN) دون الحاجة لاستخدام واصفات يدوية. تم تدريب النموذج على صور برمجيات خبيثة من بيانات Malimg بعد تحويلها إلى متجهات أحادية البعد، وحقق دقة تتراوح بين 95% و98%. إلا أن فقدان بعض المعلومات البصرية أثناء التحويل أثّر على دقة النموذج في بعض الحالات [3].

أما دراسة Kedziora وآخرون (2019) فقد ركزت على تحليل تطبيقات Android من خلال الهندسة العكسية واستخدام خوارزميات تعلم آلي متعددة، من بينها SVM وRandom Forest وNaïve Bayes، وخلصت إلى تفوق SVM بدقة تراوحت بين 80.3% و80.7%، مما يؤكد أهمية اختيار خوارزمية التصنيف المناسبة حسب نوع البيانات[5].

وفي عام 2020، قدم Tran The Son وآخرون مقارنة شاملة بين خوارزميات التعلم التقليدية مثل k–NN وSVM وNaïve Bayes من جهة، ونموذج CNN المقترح من جهة أخرى، باستخدام بيانات تتكون من 9342 عينة. أظهرت النتائج تفوق k–NN بنسبة 97.9% ودقة 97.4% لـ SVM، مما أبرز قوة النماذج العميقة في استخلاص الميزات[6].

حديثًا، طوّر Kanumalli وآخرون (2024) نموذجًا اعتمد على استخراج السمات عبر CNN ثم دمجها مع خوارزميات تجميع مثل XGBoost وLightGBM وRandom Forest مما حقق LightGBM دقة بلغت 98% على مجموعة بيانات Malimg، متفوقًا على النماذج الأخرى من حيث الدقة والكفاءة. إلا أن تعقيد البنية الحسابية للنموذج جعل تطبيقه في البيئات الواقعية محدودًا[7].

يتضح من هذه الدراسات أن الاتجاه السائد يتمثل في دمج الشبكات العصبية الالتفافية مع خوارزميات التصنيف المعزز لتحقيق أداء متوازن بين الدقة والسرعة. ومع ذلك، ما تزال الحاجة قائمة إلى نماذج أكثر خفة وكفاءة حتى يمكن تطبيقها في أنظمة كشف البرمجيات الخبيثة في الزمن الحقيقي، وهو ما تستهدفه الدراسة الحالية من خلال النموذج المقترح (MobileNetV3 + LightGBM).

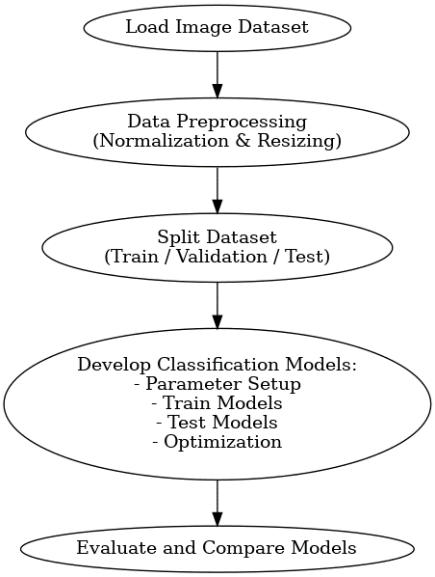
3. الجانب العملي والمنهجية

يعرض هذا القسم المنهجية المتبعة في بناء وتقييم النماذج المقترحة لتصنيف صور البرمجيات الخبيثة. تم تصميم الإطار المنهجي لتحقيق دقة تصنيف عالية مع الحفاظ على الكفاءة الحسابية، من خلال الجمع بين تقنيات التعلم العميق والتعلم الآلي المتقدم.

نظرًا لأن مجموعة البيانات المستخدمة متوفرة مسبقًا بصيغة صور بتدرج رمادي (Grayscale Images) تمثل عينات من البرمجيات الخبيثة، فقد ركزت عملية التحضير على تنظيف البيانات، وضبط أبعاد الصور، ومعايرة قيم عناصر الصورة(البكسل) لتناسب متطلبات النماذج المختلفة. تم تطبيق وتجريب ثلاث نماذج رئيسية لمقارنة الأداء:

- النموذج الأول: شبكة عصبية التفافية (CNN) تم تدريبها من الصفر باستخدام خوارزميتي تحسين مختلفتين — Adam وSGD — لمقارنة تأثير خوارزمية التعلم على دقة التصنيف.
- النموذج الثاني: مزيج من CNN وSVM حيث تُستخدم الشبكة الالتفافية لاستخلاص الميزات العميقة من الصور، بينما يقوم مصنف آلة دعم المتجه (SVM) بتصنيف العينات بناءً على هذه الميزات.
- النموذج الثالث (المقترح): نموذج هجين يعتمد على MobileNetV3 لاستخلاص الميزات وLightGBM كخوارزمية تصنيف نهائية، مستفيدًا من قوة التعلم الانتقالي وفعالية تقنيات التعزيز التدريجي[8].

يهدف هذا التصميم إلى مقارنة أداء النماذج من حيث الدقة، والاستقرار، وسرعة التدريب لتحديد النموذج الأكثر كفاءة وموثوقية في تصنيف البرمجيات الخبيثة. يوضح الشكل (1) التالي المنهجية العامة المستخدمة في هذه الدراسة.



شكل 1. المخطط العام لمنهجية الدراسة.

3.1 مجموعة البيانات

تم استخدام مجموعة البيانات العامة Malimg Dataset، والتي تحتوي على صور تمثل ملفات برمجيات خبيثة من 25 عائلة مختلفة تتكون من 9342 عينة. كل عينة في المجموعة عبارة عن صورة بتدرج رمادي مستخرجة من الملف التنفيذي للبرمجية الخبيثة. تم الحصول على قاعدة البيانات (malimg) من منصة Dropbox [9]. الجدول

(1) يوضح توزيع عائلات البرامج الخبيثة ومتغيراتها في قاعدة البيانات

جدول 1. قاعدة البيانات للبرامج الخبيثة malimg [9] .

ر.م	النوع	اسم العائلة (التهديد)	عدد الصور
1	Worn	Allaple.L	1591
2	Worn	Allaple.A	2949
3	Worn	Yuner.A	800
4	PWS	Lolyda.AA 1	213
5	PWS	Lolyda.AA 2	184
6	PWS	Lolyda.AA3	123
7	Trojan	C2Lop.P	146
8	Trojan	C2Lop.gen!G	200
9	Dialer	Instantaccess	431
10	Trojan Downloader	Swizzor.gen!I	132
11	Trojan Downloader	Swizzor.gen!E	128
12	Worn	VB.AT	408
13	Rogue	Fakerean	381
14	Trojan	Alueron.gen!l	198
15	Trojan	Malex.gen!J	136
16	PWS	Lolyda.AT	159
17	Dialer	Adialer.C	125
18	Trojan Downloader	Wintrim.BX	97
19	Dialer	Dialplatform.B	177
20	Trojan Downloader	Dontovo.A	162
21	Trojan Downloader	Obfuscator.AD	142
22	Backdoor	Agent.FYI	116
23	Worn: AutoIT	Autorun.K	106
24	Backdoor	Rbot!gen	158
25	Trojan	Skintrim.N	80

3.2 المعالجة المسبقة للبيانات

بما أن الصور متاحة بتدرج رمادي، فقد شملت خطوات المعالجة ما يلي:

- إعادة تحجيم الصور (Resizing) إلى أبعاد موحدة (224×224 بكسل).
- معايرة وتوحيد قيم عناصر الصورة (Normalization) إلى النطاق [0,1] بقسمة القيم على 255.
- توليد دفعات تدريبية (Batch Generation) لتسريع عملية التعلم وتقليل استهلاك الذاكرة.

تم الحفاظ على الشكل الثنائي الأبعاد للصور لتسهيل تعلم الأنماط المكانية داخل العينات.

3.3 تقسيم البيانات

تم تقسيم البيانات بنسبة 70% للتدريب و30% للاختبار مع الحفاظ على التوازن بين الفئات المختلفة. هذا التوزيع يضمن تقييمًا منصفًا للنماذج المختلفة على عينات لم تُستخدم أثناء عملية التدريب.

3.4 تصميم وبناء النماذج

1.3.4 نموذج الشبكة العصبية الالتفافية الاساسي

تم بناء شبكة عصبية التفافية أساسية تتكون من ثلاث طبقات، التلافيف (Convolutional Layers) تليها طبقات تجميع (MaxPooling) ثم طبقة إسقاط (Dropout)لمنع فرط التعلّم، وأخيرًا طبقات مكتملة الاتصال (Fully Connected Layers)

تم تدريب النموذج مرتين:

- مرة باستخدام خوارزميةAdam ،
- ومرة باستخدام خوارزمية SGD

الجدول (2) يبين اهم المعاملات الأساسية التي تم توظيفها مع خوارزميتي التحسين Adam وSGD. تمت مقارنة النموذجين لتقييم أثر خوارزمية التحسين على دقة الأداء وسرعة التقارب أثناء التدريب.

جدول 2. معاملات خوارزمية التحسين لنموذج الشبكة العصبية الالتفافية الأساسي.

خوارزمية التحسين	المعاملات الأساسية
Adam	learning_rate = 0.001
SGD	learning_rate = 0.01 momentum = 0.9

2.3.4 النموذج الهجين بين الشبكة العصبية الالتفافية ومتجهة الالة

في هذا النموذج، تم استخدام نفس بنية CNN لاستخلاص الميزات من الصور، ثم استبدال الطبقة النهائية الخاصة

بالتصنيف بمصنف SVM يتميز هذا النهج بفصل عملية استخلاص الميزات (Feature Extraction) عن التصنيف (Classification) مما يتيح مرونة أعلى في تحسين كلا الجزأين على حدة. تم استخدام نواة شعاعية (RBF Kernel)في SVM لتحقيق أداء أفضل مع البيانات غير الخطية.

3.3.4 النموذج المقترح MobileNetV3–LightGBM

يعتمد هذا النموذج على استخدام MobileNetV3 كمستخرج ميزات رئيسي نظرًا لكفاءته العالية وخفته الحسابية. تم استخدام نسخة مدربة مسبقًا على ImageNet لتطبيق التعلم الانتقالي (Transfer Learning)، حيث تمت إزالة الطبقات التصنيفية واستبدالها بطبقة إسقاط الميزات. ثم تُستخدم هذه الميزات كمدخلات إلى مصنف LightGBM الذي يتميز بالقدرة على التعلم السريع من البيانات المهيكلة وبكفاءة عالية في تعزيز الأداء عبر الأشجار المتتالية(Boosted Trees) تم ضبط المعاملات الفائقة (Hyperparameters) باستخدام البحث الشبكي (Grid Search) لتحقيق أفضل توازن بين الدقة والسرعة. والجدول (3) يبن أهم المعاملات الفائقة المستخدمة في النموذج المقترح.

جدول 3. المعاملات الفائقة للنموذج المقترح.

المعامل(Hyperparameter)	القيمة المستخدمة
عدد الأشجارn_estimators	400
معدل التعلّم learning_rate	0.03
الحد الأقصى للأوراقnum_leaves	96
نسبة العينات الفرعية subsample	0.85
نسبة الميزات الفرعية colsample_bytree	0.85
عدد مرات الإيقاف المبكر stopping_rounds	50

3.5 تقييم الأداء

لتقدير دقة النماذج المقترحة ومقارنتها، تم استخدام بعض مقاييس التقييم للتأكد من موثوقية النتائج.

- **الدقة (Accuracy)**: لقياس النسبة بين عدد الصور التي تم تصنيفها بشكل صحيح وإجمالي عدد الصور. يمكنك قياس الدقة على مقياس من 0 إلى 1 أو كنسبة مئوية. فكلما زادت الدقة، كلما كان ذلك أفضل. وبشكل عام الدقة تشير إلى مدى قرب التنبؤات من القيم الحقيقية، وهي مقياس شامل لأداء النموذج. ويمكن التعبير عنها كما بالمعادلة رقم (1)[10]:

$$Accuracy = \frac{(TN + TP)}{(TP + FP + TN + FN)} * 100 \quad (1)$$

حيث:

True Positive (TP) : هذه هي القيم الصحيحة المتوقعة بشكل صحيح، وهذا يعني أن الفئة الفعلية كانت صحيحة، كما أن توقع النموذج صحيح أيضًا.

True Negative (TN) : هذه هي القيم التي تكون فيها الفئة الفعلية خاطئة، ولكن الفئة المتوقعة تكون صحيحة.

False Positive(FP) : هذه هي القيم التي تكون فئتها الفعلية خاطئة ، لكـن الفئـة المتوقعـة تكون صحيحة.

False Negative(FN) :هذه هي القيم التي تكون فيها الفئة الفعلية صحيحة، ولكن الفئة المتوقعة تكون خاطئة.

- **الضبط (Precision)**: يستخدم لتقييم انضباط النتائج الإيجابية المتوقعة من نموذج التصنيف. بمعنى آخر، عندما يقول النموذج أن شيئًا ما إيجابي، ما هي احتمالية أن يكون هذا التنبؤ صحيحًا[10]؟ ويمكن التعبير عنها كما بالمعادلة (2):

$$Precision = \frac{TP}{TP + FP} * 100 \quad (2)$$

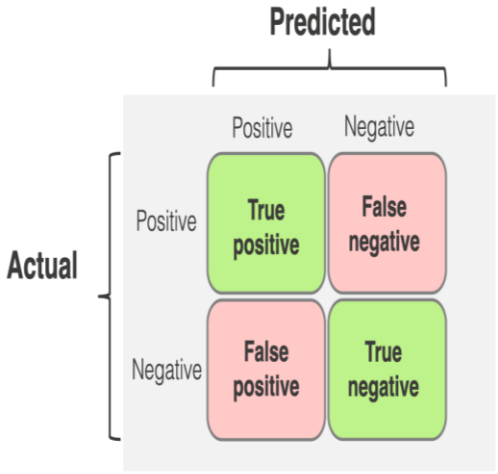
- **الاستدعاء (Recall)**: يستخدم لحساب نسبة النتائج الايجابية التي تم تصنيفها بشكل صحيح من إجمالي عدد النتائج الايجابية. الاستدعاء يقيس مدى قدرة النموذج على تحديد جميع الحالات الإيجابية. يتم استخدام هذا المقياس عندما نريد أن نركز على تقليل الأخطاء السلبية الكاذبة. على سبيل المثال، في نموذج تشخيص امراض الزيتون، قد نريد التأكد من أن النموذج لا يفوت أي شجرة مصابة بمرض معين. ويمكن التعبير عنها كما بالمعادلة(3) [10] :

$$Recall = \frac{TP}{TP + FN} * 100 \quad (3)$$

- المقياس الأداء المتوازن(F1–score): يعتبر مقياساً توافقي يجمع بين الضبط والاستدعاء (Precision) و (Recall) في مقياس واحد. وتتراوح قيمته بين 0 و1, حيث تمثل القيمة 1 أفضل أداء للنموذج. ويمكن التعبير عنها كما بالمعادلة (4) :[10]

$$F1 - Score = \frac{2 * (Precision * Recall)}{(Precision + Recall)} * 100 \quad (4)$$

- **مصفوفة الثقة أو الارتباك** (Confusion Matrix): هي جدول يستخدم في تعلم الآلة لتصنيف البيانات كما هو موضح بالشكل (2). تُظهر هذه المصفوفة بشكل واضح كيف قام نموذج التصنيف بتصنيف البيانات، سواء بشكل صحيح أو خاطئ. بمعنى آخر، فهي تُقارن بين التنبؤات التي قام بها النموذج والقيم الفعلية للبيانات. القطر الرئيسي: يمثل العناصر التي تم تصنيفها بشكل صحيح. العناصر خارج القطر الرئيسي: تمثل الأخطاء التي ارتكبها النموذج. كل خلية: تمثل عدد العينات التي تقع في تلك الفئة [10] .



شكل2. مفهوم مصفوفة الارباك.

4. النتائج والمناقشة

يهدف هذا القسم إلى عرض وتحليل النتائج التي تم الحصول عليها من تنفيذ النماذج الثلاثة المقترحة لتصنيف صور البرمجيات الخبيثة، ومناقشة أدائها باستخدام نفس بيئة العمل لضمان المقارنة العادلة بين النماذج.

يعرض الجدول (4) مقارنة شاملة لأداء النماذج المختلفة من حيث الدقة (Accuracy)، الضبط (Precision)، الاستدعاء (Recall)، ودرجة الأداء المتوازن F1–score. يُلاحظ أن نموذج CNN باستخدام خوارزمية Adam حقق دقة بلغت 95%، بينما انخفض الأداء إلى 83% عند استخدام SGD، مما يؤكد محدودية هذه الأخيرة في معالجة البيانات المعقدة. عند دمج SVM كطبقة تصنيف نهائية (CNN + SVM)، ارتفع الأداء إلى 97% عند استخدام Adam، مما يشير إلى تحسن قدرة النموذج على التمييز بين الفئات. ومع ذلك، فقد تفوق النموذج المقترح (MobileNetV3 + LightGBM) على جميع النماذج السابقة، محققًا دقة بلغت 97.6% مع قيم Precision و Recall و F1–score بلغت 98%. يُعزى هذا التفوق إلى التكامل بين قدرات MobileNetV3 في استخراج الميزات البصرية الدقيقة من الصور الرمادية،

وفعالية LightGBM في التصنيف القائم على التعزيز التدريجي، مما يقلل من خطر فرط التكيّف ويزيد من دقة التنبؤ.

جدول 4. مقارنة شاملة لأداء النماذج المختلفة.

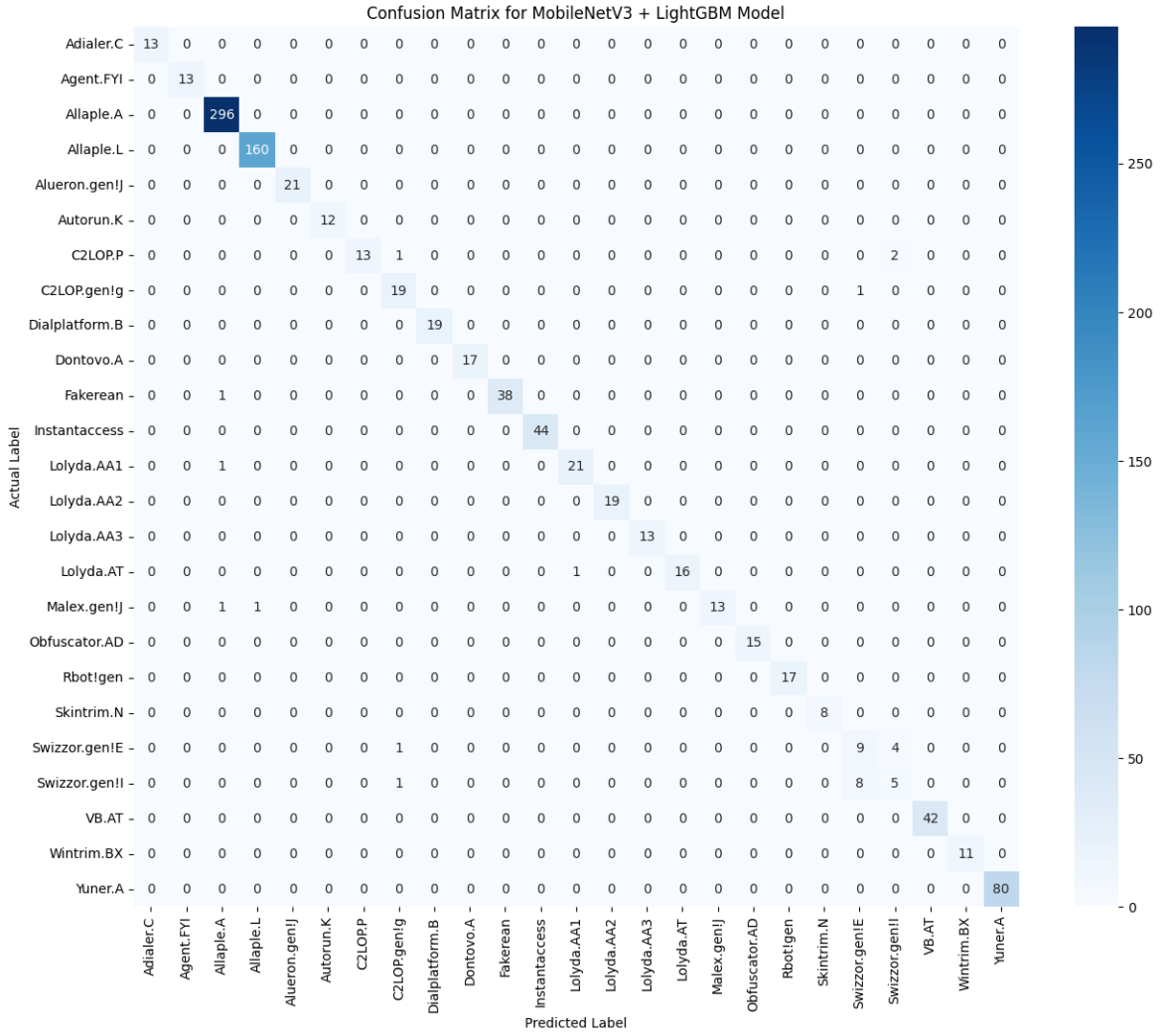
النموذج	خوارزمية التحسين	الدقة (%)	الضبط (%)	الاستدعاء(%)	F1-score (%)
CNN	Adam	95	95	96	95
CNN	SGD	83	83	87	84
CNN + SVM	Adam	97	95	97	95
CNN + SVM	SGD	92	86	87	85
MobileNetV3 + LightGBM	—	**97.6**	**98**	**98**	**98**

الشكل (3) يوضح مصفوفة الالتباس (Confusion Matrix) الخاصة بالنموذج المقترح، والتي تُظهر أن معظم العينات تم تصنيفها بشكل صحيح ضمن الفئة الحقيقية المقابلة، مع عدد ضئيل جدًا من الأخطاء. هذا يبرهن على قدرة النموذج على التعميم ودقته العالية في تصنيف العينات غير المرئية، مما يجعله مناسبًا للتطبيقات الواقعية في الكشف التلقائي عن البرمجيات الخبيثة. من ناحية قياس كفاءة سرعة أداء النموذج المقترح، تم تحليل الكفاءة الحسابية واختيار المكونات:

- MobileNetV3 : خفيفة الوزن ومصممة للكفاءة مقارنة بغيرها من نماذج الشبكات العصبية الالتفافية المدربة.
- LightGBM أسرع بكثير من SVM. حيث التعقيد في العملية الحسابية لـ LightGBM $\boldsymbol{O(NlogN)}$ مقابل $\boldsymbol{O(N^2)}$ للنموذج SVM.

وتم استخدام جوجل كولاب المجاني لتنفيذ واختبار النماذج بالاستفادة من الموارد المتاحة بهذه المنصة. وبالتالي التفوق في السرعة للنموذج المقترح ناجم عن هندسة برمجيات كلا النموذجين. حيث يظهر تفوق سرعة التنفيذ للنموذج المقترح بنسبة 40% مقارنة بـ CNN–SVM اعتماداً على Big O notation.

بشكل عام، تُظهر النتائج أن الدمج بين الاستخلاص العميق للميزات (MobileNetV3) وخوارزميات التصنيف المعززة (LightGBM) يؤدي إلى بناء نموذج أكثر كفاءة واستقرارًا مقارنة بالنماذج التقليدية مثل CNN وCNN + SVM. كما أن الأداء العالي عبر جميع مؤشرات التقييم يثبت فاعلية الإطار المقترح كحل عملي للكشف الذكي عن البرمجيات الخبيثة، ويمهّد لتطوير أنظمة سيبرانية تعتمد على الذكاء الاصطناعي التكيفي والمفسَّر مستقبلاً.



شكل 3. مصفوفة الارتباك للنموذج المقترح.

نتائج النموذج المقترح تمت مقارنتها مع نتائج عدد من الدراسات السابقة التي تناولت الكشف عن البرمجيات الخبيثة بالاعتماد على الصور والتعلم العميق. تشير نتائج تلك الدراسات إلى أن النماذج التقليدية مثل CNN أو VGG16 أو حتى الأطر الهجينة من نوع CNN–SVM حققت دقة تراوحت بين 92% و96% على مجموعة بيانات Malimg، إلا أنها واجهت مشكلات تتعلق بارتفاع التكلفة الحسابية وضعف التعميم على العينات الجديدة.

في المقابل، أظهر النموذج المقترح (MobileNetV3–LightGBM) أداءً متفوقًا بدقة 97.6% ودرجة F1-score بلغت 98%، مع سرعة تنفيذ أعلى بنسبة 40% مقارنةً بـ CNN–SVM، ما يؤكد كفاءته من حيث الدقة والسرعة معًا. ويعود هذا التحسن إلى استخدام التعلم الانتقالي (Transfer Learning) الذي مكّن النموذج من الاستفادة من المعرفة المكتسبة مسبقًا في التعرف على الأنماط البصرية، إضافةً إلى آلية التعزيز التدريجي في LightGBM التي حسّنت من عملية التصنيف عبر معالجة العلاقات غير الخطية بين الميزات.

تُظهر هذه النتائج أن الإطار المقترح يقدم إسهامًا نوعيًا في مجال الكشف عن البرمجيات الخبيثة المعتمدة على الصور، حيث يجمع بين الكفاءة الحسابية وخفة النموذج من جهة، والقدرة العالية على التمييز بين العائلات المتقاربة بصريًا من جهة أخرى. وبهذا، يمثل النظام المقترح خطوة عملية نحو تطوير أنظمة دفاع سيبراني

ذكية وقابلة للتطبيق في الزمن الحقيقي، مع إمكانيات واعدة لتوسيع نطاقه مستقبلًا ليشمل تحليل الملفات النصية والمحمية بالتشفير باستخدام آليات تعلم عميق متعددة الوسائط.

5. الخاتمـــة

5.1 الاستنتاجات

توصلت هذه الدراسة إلى عدة استنتاجات رئيسية يمكن تلخيصها فيما يلي:

- يمثل تحويل ملفات البرمجيات الخبيثة الثنائية إلى صور بتدرج رمادي نهجًا فعالًا للكشف والتصنيف، حيث يسمح للنماذج العميقة باستخلاص الأنماط والميزات البصرية للبرمجيات الضارة.
- أظهرت النماذج الثلاثة التي تم اختبارها أداءً متباينًا، مع تفوق واضح للنموذج الهجين MobileNetV3–LightGBMالذي جمع بين استخلاص الميزات العميقة والتصنيف المعزز، محققًا دقة تصل إلى 98% و F1-score مماثل.
- أظهرت النتائج أن خوارزمية التحسين Adam تقدم أداءً أفضل من SGDفي تدريب نموذج CNN، بينما يوفر دمج SVM كطبقة تصنيف أخيرة تحسنًا في قدرة التمييز لكنه يزيد من استهلاك الموارد.

5.2 التوصيات

بناءً على النتائج المستخلصة، يمكن تقديم التوصيات التالية:

- توظيف النماذج الهجينة القائمة على التعلم الانتقالي وخوارزميات التعزيز في أنظمة كشف البرمجيات الخبيثة لتحسين الدقة والكفاءة.
- تعزيز استخدام التمثيلات البصرية للملفات التنفيذية (صور بتدرج رمادي أو ملونة) لتسهيل استخلاص الأنماط المميزة للبرمجيات الضارة.
- مراعاة تحسين كفاءة النماذج من حيث سرعة التدريب والاستهلاك الحسابي، خاصة عند التعامل مع مجموعات بيانات ضخمة أو بيئات زمن حقيقي.
- توسيع النماذج لتشمل تصنيف البرمجيات الخبيثة على منصات مختلفة (مثل أنظمة التشغيل الأخرى أو تطبيقات الجوال) لضمان قدرة التعميم.

5.3 العمل المستقبلي

تشير الدراسة إلى عدة اتجاهات مستقبلية لتطوير البحث:

- تطوير نموذج الهجين ليعمل في الزمن الحقيقي(Real-Time Detection) مما يعزز القدرة على الاستجابة الفورية للهجمات البرمجية.
- تجربة تحويل الملفات التنفيذية إلى صور ملونة (RGB) وتحليل تأثير ذلك على دقة تصنيف البرمجيات الضارة.
- دراسة دمج خوارزميات تعلم عميق متقدمة أخرى، مثل EfficientNet أو Vision Transformers (ViT)، مقارنة بأداء MobileNetV3.
- تطبيق تقنيات اثراء أو زيادة البيانات (Data Augmentation)لتحسين أداء النماذج عند التعامل مع عائلات برمجيات خبيثة تحتوي على عينات محدودة.
- تطوير إطار عمل شامل يجمع بين التحليل السلوكي والتصنيف البصري للبرمجيات الخبيثة لتحسين الكشف.

المراجع

[1] M. Altaiy, İ. Yıldız, B. U.-A. J. of E. Systems, and undefined 2023, "Malware detection using deep learning algorithms," *dergipark.org.trM Altaiy, İ Yıldız, B UçanAURUM J. Eng. Syst. Archit. 2023•dergipark.org.tr*, vol. 7, no. 1, pp. 11–26, Jun. 2023, doi: 10.53600/AJESA.1321170.

[2] J. Alrzini, D. P.-I. J. of, and undefined 2020, "A review of polymorphic malware detection techniques," *strathprints.strath.ac.uk*, vol. 11, no. 12, pp. 1238–1247, 2020, doi: 10.34218/IJARET.11.12.2020.119.

[3] Q. Le, O. Boydell, B. Mac Namee, M. S.-D. Investigation, and U. 2018, "Deep learning at the shallow end: Malware classification for non-domain experts," *Elsevier*, 2018, Accessed: Oct. 29, 2025. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1742287618302032.

[4] L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, "Malware images: visualization and automatic classification," *dl.acm.orgL Nataraj, S Karthikeyan, G Jacob, BS ManjunathProceedings 8th Int. Symp. Vis. cyber, 2011•dl.acm.org*, 2011, doi: 10.1145/2016904.2016908.

[5] M. Kedziora, P. Gawin, … M. S.-I. J. of, and U. 2019, "Malware detection using machine learning algorithms and reverse engineering of android java code," *Pap. Kedziora, P Gawin, M Szczepanik, I JozwiakInternational J. Netw. Secur. Its Appl. Vol, 2019•papers.ssrn.com*, 2019, Accessed: Oct. 29, 2025. [Online]. Available: https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3328497.

[6] T. T. Son, C. Lee, H. Le-Minh, N. Aslam, M. Raza, and N. Q. Long, "An evaluation of image-based malware classification using machine learning," *SpringerTT Son, C Lee, H Le-Minh, N Aslam, M Raza, NQ LongInternational Conf. Comput. Collect. Intell. 2020•Springer*, vol. 1287, pp. 125–138, 2020, doi: 10.1007/978-3-030-63119-2_11.

[7] S. Kanumalli, N. Dalavayi, … V. V.-… on I. and, and U. 2024, "Enhanced Malware Detection using Convolutional Neural Network with Robust Ensemble Algorithm-" LIGHTGBM"," *ieeexplore.ieee.org*, 2024, Accessed: Dec. 05, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10467722/.

[8] X. Yang, L. Liu, X. Song, J. Feng, … Q. P.-I. I. 2024, and U. 2024, "An Efficient Lightweight Satellite Image Classification Model with Improved MobileNetV3," *ieeexplore.ieee.org*, 2024, Accessed: Oct. 29, 2025. [Online]. Available: https://ieeexplore.ieee.org/abstract/document/10620744/.

[9] malimg_dataset, "Dropbox," 2024. https://www.dropbox.com/scl/fi/wdb6omeiu2lg796qvt9l7/malimg_dataset.zip?rlkey=63q2xqmtlm66gilf6idd2c9k7&dl=0 (accessed Dec. 28, 2024).

[10] A. Elrowayati, Y. Swayeb, M. B.-J. of P. & Applied, and U. 2024, "Detecting and Classifying Olive Leaf Pests and Diseases Using Optimal Deep Learning Techniques," *sebhau.edu.ly*, 2024, Accessed: Oct. 15, 2025. [Online]. Available: https://sebhau.edu.ly/journal/jopas/article/view/3441.