Journal of Autonomous Intelligence (2024) Volume 7 Issue 5
doi: 10.32629/jai.v7i5.1287

ORIGINAL RESEARCH ARTICLE

A recent survey of image-based malware classification using convolution neural network

Kennedy E. Ketebu[1], Gregory O. Onwodi[1], Kingsley Eghonghon Ukhurebor[2,*], Benjamin Maxwell Eneche[1], Nana Kojo Yaah-Nyakko[3]

[1] *Africa Centre of Excellence on Technology Enhanced Learning (ACETEL), National Open University of Nigeria, Abuja 900001, Nigeria*

[2] *Department of Physics, Edo State University Uzairue, Auchi 312001, Edo State, Nigeria*

[3] *Department of Computer Science, Kwame Nkrumah University of Science and Technology, Kumasi 03220, Ghana*

*** Corresponding author:** Kingsley Eghonghon Ukhurebor, ukeghonghon@gmail.com

ABSTRACT

Despite numerous breakthroughs in creating and applying new and current approaches to malware detection and classification, the number of malware attacks on computer systems and networks is increasing. Malware authors are continually changing their operations and activities with tools or methodologies, making it tough to categorize and detect malware. Malware detection methods such as static or dynamic detection, although useful, have had challenges detecting zero-day malware and polymorphic malware. Even though machine learning techniques have been applied in this area, deep neural network models using image visualization have proven to be very effective in malware detection and classification, presenting better accuracy results. Hence, this article intends to conduct a survey showing recent works by researchers and their techniques used for malware detection and classification using convolutional neural network (CNN) models highlighting strengths, and identifying areas of potential limitations such as size of datasets and features extraction. Furthermore, a review of relevant research publications on the subject is offered, which also highlights the limitations of models and dataset availability, along with a full tabular comparison of their accuracy in malware detection and classification. Consequently, this review study will contribute to the advancement and serve as a basis for future research in the field of developing CNN models for malware detection and classification.

Keywords: convolution neural network; datasets; machine learning; malware; visualization

ARTICLE INFO

Received: 26 September 2023
Accepted: 18 October 2023
Available online: 7 March 2024

1. Introduction

The continuous and rapid advancement in technology and its pervasive use in processing and managing information have ushered in a new era of diverse digital threats[1]. Modern-day computer attacks or cyberattacks are on the increase and becoming more complex, with the increasing number of computers and mobile devices connected to the internet or cyberspace and users accessing various digital mediums or platforms. However, this has made users, computers, and networks vulnerable to various types of attacks on the internet or in a computer environment. Malicious software, also known as malware, are harmful programs that expose or steal sensitive data or information, as well as compromises the integrity of a computer system by preventing it from operating securely.

Malware attacks are a major source of concern for individuals and cybersecurity experts, as they have resulted in denial of services, loss of privacy, intellectual property, and financial losses for victims and organizations all over the world. Machine learning techniques have

been effective in malware detection and classification; however, attackers attempt to disguise malware as legitimate files using techniques such as packing, encryption, and polymorphism; this may result in the pre-trained model making incorrect predictions[2]. Recent malware attacks have become more sophisticated as a result of the use of machine learning. It is estimated that at least 230,000 malware samples are produced every day, and 18 million websites are infected with malware each week[3].

In developing effective malware detection and classification engines, there are two main methods, namely static and dynamic analysis. Machine learning approaches have been applied in malware analysis. The two main approaches, which are static and dynamic, differ from each other in the manner in which features are extracted statically or dynamically (runtime execution)[4]. There are various similar variations of malware samples. This is because malware authors reuse the previous codes, only making changes so as to form or develop new malware samples[5]. Newer methods are being developed towards malware classification and detection; one of such areas is the area of visualization. Visualization techniques have been effective in enabling and understanding complex data analytics[6], or structures. One of the first researcher to use visualization was Nataraj et al.[7], who represented malware samples as grayscale images in order to distinguish similarities and differences among malwares samples. This showed visual similarities of malwares belonging to the same family.

Visualization can greatly aid malware classification and does not necessitate any disassembly (static analysis) or code execution (dynamic analysis)[5]. This is because performing feature extractions of malware samples requires a degree of expert domain knowledge when performing either static or dynamic analysis. However, researchers have found that deep learning can produce better performance when compared to existing machine learning approaches or methods[8]. Deep learning computational approach has been successful in solving complex computational tasks, this is because of its ability to learn massive amounts of data thereby outperforming other machine learning techniques in different domains such as bioinformatics, language processing, cybersecurity, robotics, control systems and many others[9].

One of the main advantages of deep learning is its ability to execute feature engineering on its own by scanning the dataset for features that corelate with each other so as to enable faster learning. Due to the increase rate of malware attacks, it has become very critical in how malwares are quickly identified and classified. Traditional machine learning methods are limited by feature engineering and size of data being processed; hence Deep learning has become an effective solution[10]. Recently, researchers have begun the use of deep learning models towards classification of malware[11], which also has a higher predictive accuracy. Hence deep learning using neural network model is being applied towards classification of malwares. At the current rate deep learning neural network has grown to the state to surpass the limitation of machine learning techniques, this is because of the possibility of using deep learning to develop models with significantly higher number of diverse layers[12].

The increase in the use of visualization of malwares into images for malware classification employing convolutional neural networks (CNN) models has been successful in detecting and classifying malwares. However, given the evolving trend in malwares and the susceptibility of deep learning models to adversarial attacks, there is a need to critically study recent efforts by researchers in developing image-based malware classification models. Hence, this survey presents a brief but yet an all-inclusive analysis of recent research works mostly from 2018 to date and its innovations in malware classification using CNN models. It also discusses the challenges faced in development of image-based malware classification models. The main goal of this paper is to present an overview on recent advancements by researchers in malware classification using CNN models, highlighting strengths, and identifying areas of potential limitations such as size of datasets and features extraction. Consequently, this review study will contribute to the advancement and serve as a basis for future research in the field of developing CNN models for malware detection and classification.

This paper is organized into the following sections, Section 1 which having be discussed already is the introduction, Section 2 takes a look at the recent works by researchers who develop CNN models for efficient and effective identification and classification of malwares, as well as tabular comparison of the models. In Section 3, a detailed analysis is done which identifies the issues and challenges of the CNN models used. Section 4 concludes this review with recommendations for future perspectives.

2. Related works

The utilization of image based (CNN) models for malware classification has experienced a significant increase in prominence over recent years[13]. This section offers a comprehensive analysis of recent research in this domain, summarizing key findings and outlining limitations identified within the various researchers' works.

Kalash et al.[8] proposed a deep learning framework for malware classification using deep CNN architecture, which is referred to as M-CNN model. The model processes grayscale images of 2binaries from two datasets (Malimg and Microsoft malware dataset). The result of the experiments achieved an accuracy score of 98.52% and 99.7% on Malimg and Microsoft malware dataset respectively.

In a research work by Le et al.[14], using the Microsoft malware classification challenge dataset, a model was developed which combines a CNN plus two bi-directional long short-term memory architectures (CNN-BiLSTM) for malware classification. A generic image scaling algorithm which interprets the malware file byte code as a one-dimensional (1-D) image with a fixed target size. The generated images are fed to the CNN-BiLSTM model in which the output of convolutional layers is connected to one forward LSTM layer and one backward layer. The two outputs are then fed to the output layer of the model, the result of model achieved an average accuracy score of 98.8%. Although the model was effective, it was slower than an average CNN model.

In a research work by Lo et al.[15], the researchers performed malware classification using a special CNN architecture Xception model based which its experiment was based on Malimg and Microsoft malware dataset. This approach performs malware classification using two file types (.byte and .asm) in which the predictions are stacked together so as to give a predictive result. This helps to reduce overfitting problem as well as achieved a very high accuracy 99.03%. The Xception model was very effective and less time consuming when compared to other methods such as KNN, SVM and VGG16.

Vasan et al.[16], proposed a technique they named "Image-based Malware Classification using Ensemble of CNNs (IMCEC)" (see **Figure 1** for an outline of the proposed IMCEC). The basic premise is that several CNNs produce distinct semantic representations of the picture according to their deeper designs; hence, a collection of CNN architectures enables the extraction of features with better quality than can be achieved with conventional techniques. The outcomes of the experiments indicate that IMCEC is especially well-suited for detecting malware. Using malware raw input, it can achieve low false alarm rates and excellent detection accuracy. The outcome shows that over 99% of malware that has been unpacked and over 98% of malware that has been packed is accurately detected. IMCEC is adaptable, useful, and quick—it typically takes 1.18 seconds to detect a new malware sample.

Yoo et al.[17], proposed a machine learning hybrid model called the Al-Hydra, this model combines random forest (RF) and Multi-layered perceptron (MLP) which are very effective for malware detection. This model which consists of four sub classification models (static RF, Dynamic RF, static MLP and Dynamic MLP) uses a voting scheme in which a rule-based majority vote is used to determine if a sample is malicious or benign. The results of the experiment showed Al-Hydra having an average accuracy of 85.1% using KISA dataset.

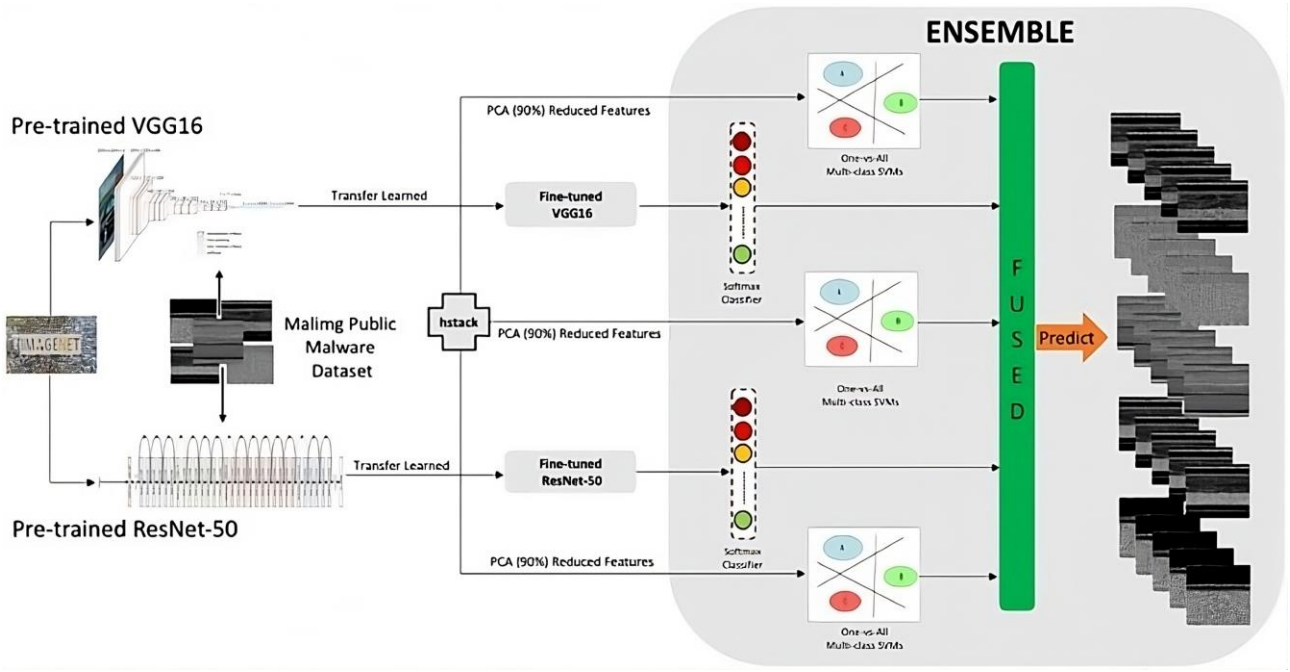

Figure 1. An outline of the proposed IMCEC.

A research work by Kumar[18], who developed a model using transfer learning called malware classification with fine-tune CNN (MCFT-CNN). This model was developed by altering the last layer with a fully connected dense layer of a pre-trained existing model ResNet50. The MCFT-CNN model when trained with Malimg dataset achieve an accuracy of 99.18% and 98.63% on Microsoft malware challenge dataset.

In another study, Awan et al.[19] proposed a model based on deep learning framework called spatial attention and CNN (SACNN) for malware classification. This model represents a simple solution which does not require generated images from binaries to undergo special preprocessing operations such as data augmentation or feature engineering in order to solve malware classification problems. The model consists of a transfer learning model (VGG19), a dynamic spatial attention mechanism which focuses on only important areas of the generated images for malware classification. The result of experiment when applied to Malimg malware dataset produced an accuracy of 97.68%.

Asam et al.[20] proposed a malware classification framework called Deep Feature Space-based malware classification (DFS-MC), the proposed model entails customizing and fine tuning ResNet-18 and DensNet-201 in combination with SVM. The hybrid model learning scheme involves extracting deep ensemble features of customized CNN models and then applying SVM classifier for malware classification on deep ensemble feature space. The proposed model produced an accuracy of 98.61%.

Carletti et al.[21], carried out an evaluation so as to determine the robustness of CNN for malware classification. This was done by specializing existing CNN models (ResNet50, InceptionV3, MobileNet and VGG16) on malware images through transfer learning for malware classification. In accessing the robustness of the models, the malware samples input is perturbed which involves subjecting the original executables through obfuscation methods. A metamorphic technique such as dead code insertion was applied directly on the hexadecimal representation of a binary file, this involves inserting junk codes into the text section of the binary file. The BIG2015 dataset used in the experiment with the experiment being in two folds with malware classification on the original dataset and accessing robustness on obfuscated dataset. The overall best CNN model was MobileNet which a high accuracy score of 99.25% and on obfuscated dataset 96.2% showing the CNN model is very robust for malware classification.

Lin and Yeh[22] proposed a bit and byte-level sequence one 1-D CNN model which extracts vital features

from the 1-D structure of binary executables, instead of converting executables into two-dimensional (2-D) images which makes it difficult to determine a fixed width with all inherited sequential structures within the byte-level sequence. Resizing and compression methods are applied to fix the length of each byte-level sequence, additionally bit transformation is applied so as to expand the byte-level to bit level sequences. This is because each machine instruction is encoded as 8 bits. The model maintains the contextual information for the machine instructions and also has fewer number of parameters in comparison to 2D CNN models. The model when applied to Microsoft malware classification challenge dataset achieved an accuracy score of 98.7% for malware classification.

In a research work by O'Shaughnessy and Sheridan[23], one area of concern was malware developers employing obfuscation techniques so as to evade detection. Hence a hybrid framework for malware classification was developed to overcome the challenges faced by other image-based malware classification models. This framework combines the strengths of both static and dynamic analysis to overcome obfuscated malware samples. This is done by converting malware samples into 2-D images mapped through space filled curve (SFC) traversals. This is important because the data structures of resulting SFC images of original malware samples are maintained after conversion. The result of the experiment when applied to the virustotal dataset gave an accuracy score of 97.6%.

Schofield et al.[24] presented a CNN model malware classification based on Windows system Application Program Interface (API) call. The researchers identified API call sequences as an important feature for malware classification, this is because API calls shows system calls or events on windows operating system occurring during runtime of a malicious file sample. The research work used a database of API call streams. The model uses both 1-D CNN and term frequency-inverse document frequency (TF-IDF) in mapping API call streams. The result of the experiment showed the 1-D CNN model achieving an accuracy score of 98.17%.

Parihar et al.[25] introduces a novel way for malware classification called stacked deep CNN (S-DNN), the model consists of three of pre-existing models which are ResNet50, Xception and EfficientNet-B4 which are trained using transfer learning and then combined to using ensemble learning techniques so as to develop a model. The developed model utilizes the combined knowledge base of the different models via ensemble learning which results in high generalization and low variance performance during malware classification. The performance of the developed model when evaluated on Malimg and Virushare dataset gave an average accuracy score of 99.43% and 99.65% respectively over ten folds.

Naeem et al.[26] introduced a novel method using CNN for the multi classification of malware families. This was done by first converting the malware binaries into sequence of pixel values producing 2-D matrix grayscale images, the CNN model uses entropy filters to find distinct patterns in the image processed. The model was evaluated using the Microsoft dataset which consist of 10,000 samples with nine distinct classifications, achieving an accuracy of 99.97%.

Ahmed et al.[27] formulated malware signatures as 2D image representation in classifying malwares using deep learning techniques on BIG 2015 dataset which contains about 10,000 samples. The model was developed using transfer learning of Inception V3 architecture and its performance produced a classification accuracy score of 98.76%. The research work compares its performance with various machine learning and deep learning technologies towards malware classification such as Logistic Regression (LR), Artificial Neural Network (ANN), CNN, transfer learning on CNN and Long Short-Term Memory (LSTM).

In a recent study, Chen and Cao[28] proposed a visualization-based malware classification system using transfer and ensemble learning (VMCTE). This model VMCTE has a strong anti-interference ability. This signifies that even if malware uses obfuscation, fuzzing, encryption, and other techniques to evade detection, it can be accurately classified into its corresponding malware family. The model combines three CNN architectures (ResNet50, MobilenetV1, and MobilenetV2) to establish the classification model. The

experimental findings on the Malimg dataset demonstrate that VMCTE can attain 99.64%, accuracy.

3. Analysis of CNN models

Numerous studies have emerged employing diverse CNN models. Some of these models have been derived from existing architectures through transfer learning, while others involve combining two or more architectures, or crafting entirely novel models from scratch. This section undertakes a comparative examination of contemporary endeavours established in the literature, focusing on both malware classification and identification using CNNs, as well as malware visualization.

In Section 2, discussion on the recent contributions documented in the literature review, which pertain to CNN-based approaches for malware classification and identification. Additionally, this section encompasses a discussion of malware visualization techniques. The comparative analysis of various CNN models, as discussed in the preceding section, is presented in **Table 1**. This analysis serves to underscore pivotal aspects including the datasets used, accuracy of the model, as well as inherent limitations.

Table 1. The malware classification models by various researchers.

Author	Classification Model	Dataset	Accuracy	Limitation
Kalash et al.[8]	M-CNN	Malimg Microsoft dataset	98.52% 99.70%	The dataset lacks robustness. Hence, the robustness of the dataset requires improvements.
Le et al.[14]	CNN-BiLSTM	Microsoft challenge dataset (BIG 2015)	98.80%	Slow training time, imbalance dataset.
Lo et al.[15]	Xception	Malimg Microsoft Malware dataset	99.03% 99.97%	The dataset lacks robustness. Hence, the robustness of the dataset requires improvements.
Yuan et al.[10]	MDMC model	Malimg Derbin Dataset	99.264% 97.364%	Processing time, the dataset lacks robustness. Hence, the robustness of the dataset and processing time require improvements.
Yoo et al.[17]	Al-hydra	KISA Dataset	85.10%	Uses high computation to extract various features, Uses voting mechanism to decide classification, this is susceptible to high false (FP) rate of begnin samples
Kumar[18]	(MCFT-CNN).	Microsoft malware challenge dataset Malimg	98.63% 99.18%	Due to the size of complex architecture of resnet50 has high computation overhead.
Awan et al.[19]	SACNN	Malimg	97.68%	Dataset imbalance, lack of the exploration in the data augmentation and the feature engineering domains.
Asam et al.[20]	DFS-MC	Malimg	98.61%	Very large processing and computation cost
Carletti et al.[21]	MobileNet Xception XGBoost	BIG2015	99.25% 99.07% 99.43%	Accuracy of models drops considerable on obfuscated samples
Lin and Yeh[22]	Byte-level 1D CNN	Microsoft malware challenge dataset	98.70%	Model did not always produce better performance while binary executables were converted and resized to larger images.
O'Shaughnessy and Sheridan[23]	SFC KNN-HOG	VirusTotal dataset	97.60%	Long conversion time of malware samples to SFC images
Parihar et al.[25]	S-DCNN	Malimg VirusShare	99.43% 99.65%	High computation time due to incorporation of the models (ResNet50, Xception, EfficientNet-B4)

Table 1. (*Continued*).

Author	Classification Model	Dataset	Accuracy	Limitation
Naeem et al.[26]	Binary code to pixel vector transformation	Microsoft malware dataset	99.97%	The dataset lacks robustness, model susceptible to overfitting
Ahmed et al.[27]	Inception V3	BIG 2015	98.76%	The dataset lacks robustness. Hence, the robustness of the dataset requires improvements.
Chen and Cao[28]	VMCTE	malimg	99.64%	High computation time due to combination of different architectures

In our investigation, we conducted a comprehensive analysis of several CNN models outlined in **Table 1**, all of which were developed by various authors for the purpose of malware classification. The graphical representation in **Figure 2** presents a bar chart illustrating the performance of these models, evaluated using accuracy metrics.

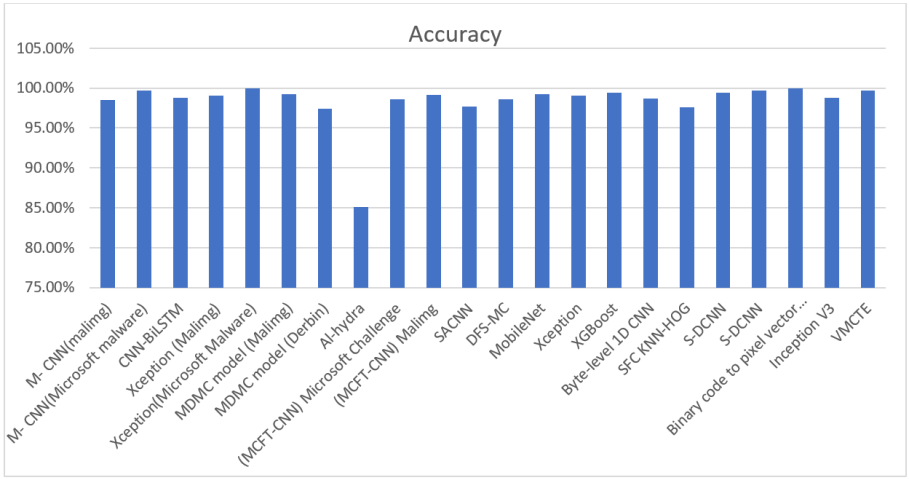

Figure 2. Bar Chart showing the accuracy of various researchers' models.

3.1. Discussion

The literature review carried out in this study delves into recent advancements in the utilization of CNN models for the image classification of malware samples. As gleaned from the insights outlined in the preceding section, it becomes apparent that among the explored CNN models, the binary code to pixel vector transformation model, when applied to the malimg dataset, achieved the highest accuracy of 99.97%. In contrast, the Al-hydra model exhibited a slightly lower accuracy score of 85.1% when operating with the KISA dataset.

Considering the datasets employed in these reviewed studies, the malimg dataset emerged as the most prevalent, featuring in eight of the investigated works. The Microsoft malware dataset, on the other hand, appeared in seven of the studies. Additionally, other datasets such as KISA, VirusTotal, and VirusShare were also used in this research.

3.2. Challenges and issues

From the review of the recent studies, several noteworthy insights have emerged, shedding light on the challenges inherent in the development of malware classification models. These identified challenges subsequently give rise to a multitude of issues within the realm of malware classification. The crux of achieving successful classification lies in the dual qualities of consistency and effectiveness in the classifier's performance. Constructing such a classifier necessitates a comprehensive consideration of all the intricacies and obstacles that are entailed. Upon closer inspection of the aforementioned studies using CNN-based approaches for malware classification reveals certain gaps and limitations which are as follows.

3.2.1. Datasets used

The datasets commonly employed by most researchers for malware classification within the reviewed literature, includes well-known datasets such as “malimg” and the “Microsoft Malware Dataset 2015” although popular among researchers they could exhibit limitations in their effectiveness when utilized for developing models that can classify newer malwares. This shortcoming arises from the fact that constructing a model based on outdated malware samples renders it ineffectual against contemporary malware threats. Consequently, the persistently evolving tactics of malware authors, who predominantly utilize modern malware samples, result in the classifiers’ inability to accurately categorize these new malicious entities.

Furthermore, these datasets suffer from a limitation of diverse malware samples. This scarcity poses a significant challenge, particularly for CNN models which thrive on substantial data volumes to achieve robust training and model development. Insufficient samples within a dataset can induce overfitting in the models, wherein they become overly specialized to the limited data and consequently fail to effectively identify novel malware instances.

3.2.2. Performance computation measures

The computational costs associated with most of these models frequently exhibit a high degree of resource consumption, sometimes with unclear correlations to their performance in malware classification. This ambiguity spans multiple facets, encompassing the definition of performance metrics, the time required for training and testing, and the intricacies of translating malware binaries into color images. Furthermore, approaches aimed at mitigating data imbalance issues during the classification of malware families, as well as efforts to condense the feature vector’s dimensions, assume noteworthy importance. This is particularly significant since the size of the feature vector significantly impacts the overall efficiency attainable by these models.

4. Conclusion and recommendations for future perspectives

This paper embarks on a brief but yet all-inclusive exploration, delving into an overview of recent innovations and comparing CNN models for the detection and classification of malware. This article conducts a survey showing recent works by researchers and their techniques used for malware detection and classification using CNN models highlighting strengths, and identifying areas of potential limitations such as size of datasets and features extraction. This review has yielded valuable insights, particularly in the domain of malware visualization using CNN architecture, which aids analysts in identifying crucial patterns. Based on the findings, it is clear that pursuing malware visualization in conjunction with the CNN approach can yield a more intelligent framework. This framework promises to enhance accuracy, efficiency, and overall performance, all of which are vital in the ever-evolving landscape of malware threats.

In the course of this review, significant knowledge gaps have been revealed, major challenges have been identified, also highlighted are open issues that will serve as valuable guides for future research endeavours.

Albeit, for future studies, the following recommendations should be considered:

1) Dataset Choice: Utilize a large, up-to-date malware dataset containing recent malware samples. This is crucial for assessing and validating performance measures effectively.
2) Image Conversion: Explore more efficient techniques for converting malware binaries into color images, considering variations in image sizes across different datasets.
3) Model Development: While transfer learning has its merits, consider focusing on the development of novel models. This approach can help mitigate errors stemming from domain mismatch, where a model trained in one domain is applied to a different one.
4) Feature Vector Dimensionality: Reduce the dimensionality of the feature vector to enhance model efficiency.

5) Data Imbalance: Implement newer methods or techniques to address data imbalance problems effectively.

Author contributions

Conceptualization, KEK, GOO and KEU; methodology, KEK, GOO and KEU; software, KEK; validation, KEK, GOO and KEU; formal analysis, KEK; investigation, KEK; resources, KEK, GOO and KEU; data curation, KEK; writing—original draft preparation, KEK and KEU; writing—review and editing, KEK, GOO, KEU, BME and NKYN; visualization, KEK, GOO and KEU; supervision, GOO and KEU; project administration, KEK, GOO and KEU; funding acquisition, KEK, GOO, KEU, BME and NKYN. All authors have read and agreed to the published version of the manuscript.

Funding

This study has not received any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Acknowledgments

The authors appreciate the authors and publishers, whose articles were used as guides for this review study. Also, the authors express gratitude to their respective institutions and the Africa Centre of Excellence on Technology Enhanced Learning (ACETEL), National Open University of Nigeria, Abuja, for supporting this study.

Data availability statement

Completely, data produced or investigated during this work were involved in this submitted article.

Conflict of interest

The authors declare no conflict of interest.

References

1. Sharma A, Gupta BB, Singh AK, et al. Orchestration of APT malware evasive manoeuvers employed for eluding anti-virus and sandbox defense. Computers & Security. 2022, 115: 102627. doi: 10.1016/j.cose.2022.102627.
2. Agrawal R, Khan L. An Experience in Enhancing Machine Learning Classifier Against Low-Entropy Packed Malwares. 2021.
3. Ghosh A. An overview article on 600% increase in Cyber Attack in 2021. 2021.
4. Gibert D, Mateu C, Planes J. The rise of machine learning for detection and classification of malware: Research developments, trends and challenges. Journal of Network and Computer Applications. 2020, 153: 102526. doi: 10.1016/j.jnca.2019.102526.
5. Moussas V, Andreatos A. Malware Detection Based on Code Visualization and Two-Level Classification. Information. 2021, 12(3): 118. doi: 10.3390/info12030118.
6. Keahey TA. Using visualization to understand big data. IBM Business Analytics Advanced Visualisation. 2013, 16.
7. Nataraj L, Karthikeyan S, Jacob G, et al. Malware images. Proceedings of the 8th International Symposium on Visualization for Cyber Security. Published online July 20, 2011. doi: 10.1145/2016904.2016908.
8. Kalash M, Rochan M, Mohammed N, et al. Malware Classification with Deep Convolutional Neural Networks. 2018 9th IFIP International Conference on New Technologies, Mobility and Security (NTMS). Published online February 2018. doi: 10.1109/ntms.2018.8328749.
9. Alzubaidi L, Zhang J, Humaidi AJ, et al. Review of deep learning: Concepts, CNN architectures, challenges, applications, future directions. Journal of Big Data. 2021, 8(1). doi: 10.1186/s40537-021-00444-8.
10. Yuan B, Wang J, Liu D, et al. Byte-level malware classification based on markov images and deep learning. Computers & Security. 2020, 92: 101740. doi: 10.1016/j.cose.2020.101740.
11. Cakir B, Dogdu E. Malware classification using deep learning methods. Proceedings of the ACMSE 2018 Conference. Published online March 29, 2018. doi: 10.1145/3190645.3190692.
12. Kolosnjaji B, Zarras A, Webster G, et al. Deep Learning for Classification of Malware System Call Sequences. Lecture Notes in Computer Science. 2016, 137-149. doi: 10.1007/978-3-319-50127-7_11.

13. Nwankwo W, Ukhurebor KE. Web Forum and Social Media: A Model for Automatic Removal of Fake Media using Multilayered Neural Networks. International Journal of Scientific & Technology Research. 2020, 9(1): 4371-4377.
14. Le Q, Boydell O, Mac Namee B, et al. Deep learning at the shallow end: Malware classification for non-domain experts. Digital Investigation. 2018, 26: S118-S126. doi: 10.1016/j.diin.2018.04.024.
15. Lo WW, Yang X, Wang Y. An Xception Convolutional Neural Network for Malware Classification with Transfer Learning. 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS). Published online June 2019. doi: 10.1109/ntms.2019.8763852.
16. Vasan D, Alazab M, Wassan S, et al. Image-Based malware classification using ensemble of CNN architectures (IMCEC). Computers & Security. 2020, 92: 101748. doi: 10.1016/j.cose.2020.101748.
17. Yoo S, Kim S, Kim S, et al. AI-HydRa: Advanced hybrid approach using random forest and deep learning for malware classification. Information Sciences. 2021, 546: 420-435. doi: 10.1016/j.ins.2020.08.082.
18. Kumar S. MCFT-CNN: Malware classification with fine-tune convolution neural networks using traditional and transfer learning in Internet of Things. Future Generation Computer Systems. 2021, 125: 334-351. doi: 10.1016/j.future.2021.06.029.
19. Awan MJ, Masood OA, Mohammed MA, et al. Image-Based Malware Classification Using VGG19 Network and Spatial Convolutional Attention. Electronics. 2021, 10(19): 2444. doi: 10.3390/electronics10192444.
20. Asam M, Khan SH, Jamal T, et al. Malware Classification Using Deep Boosted Learning. arXiv. 2021, arXiv:2107.04008.
21. Carletti V, Greco A, Saggese A, Vento M. Robustness evaluation of convolutional neural networks for malware classification. ITASEC 2021 Italian Conference on Cybersecurity. 2021, 2940: 414-423.
22. Lin WC, Yeh YR. Efficient Malware Classification by Binary Sequences with One-Dimensional Convolutional Neural Networks. Mathematics. 2022, 10(4): 608. doi: 10.3390/math10040608.
23. O'Shaughnessy S, Sheridan S. Image-based malware classification hybrid framework based on space-filling curves. Computers & Security. 2022, 116: 102660. doi: 10.1016/j.cose.2022.102660.
24. Schofield M, Alicioglu G, Binaco R, et al. Convolutional Neural Network for Malware Classification Based on API Call Sequence. Computer Science & Information Technology (CS & IT). Published online January 23, 2021. doi: 10.5121/csit.2021.110106.
25. Parihar AS, Kumar S, Khosla S. S-DCNN: Stacked deep convolutional neural networks for malware classification. Multimedia Tools and Applications. 2022, 81(21): 30997-31015. doi: 10.1007/s11042-022-12615-7.
26. Naeem MR, Amin R, Alshamrani SS, et al. Digital Forensics for Malware Classification: An Approach for Binary Code to Pixel Vector Transition. Computational Intelligence and Neuroscience. 2022, 2022: 1-12. doi: 10.1155/2022/6294058.
27. Ahmed M, Afreen N, Ahmed M, et al. An inception V3 approach for malware classification using machine learning and transfer learning. International Journal of Intelligent Networks. 2023, 4: 11-18. doi: 10.1016/j.ijin.2022.11.005.
28. Chen Z, Cao J. VMCTE: Visualization-Based Malware Classification Using Transfer and Ensemble Learning. Computers, Materials & Continua. 2023, 75(2): 4445-4465. doi: 10.32604/cmc.2023.038639.