OPEN ACCESS

Kashf Journal of Multidisciplinary Research
Vol: 02 - Issue 05 (2025)
P-ISSN: 3007-1992 E-ISSN: 3007-200X
https://kjmr.com.pk

HYBRID DEEP LEARNING EFFECTIVENESS OF IMAGE-BASED MALWARE DETECTION

Rimsha Feroz
Department of computer science, NFCIET, Multan, Pakistan.
Muhammad Ahsan Aslam
Khwaja Fareed University of Engineering and Information Technology (KFUEIT), Rahim Yar Khan.
Muhammad Fuzail
Department of computer science, NFCIET, Multan, Pakistan.

Naeem Aslam
Department of computer science, NFCIET, Multan, Pakistan.
Muhammad Kamran Abid*
Department of Computer Science, Emerson University Multan, Pakistan.

**Corresponding author: Muhammad Kamran Abid (kamran.abid@eum.edu.pk)*

Article Info

Abstract

The current high rate of malware variant production each day produces hundreds of thousands of new variants making signature detection methods ineffective. Deep learning patterns succeed at detecting malware through converting malware binaries to gray forms and detecting complex hidden patterns inside these files. CNNs and LSTMs function sub-opportunistically as standalone models to prevent new malware types. This system uses CNNs and LSTMs as components which extract spatial features through spatial extraction followed by temporal pattern processing to maximize malware classification results. The research team conducted testing operations by processing Malign and Blended datasets through images of various resolution settings. The combined network achieves 0.99 F1 score along with 0.96 accuracy that represents superior performance than the isolated individual models based on result measurements. The hybrid approach shows strong performance because it maintains effective adversarial attack resistance while maintaining high malware type recognition capabilities. According to this research the significant hurdles relate to both expensive training expenses needed to handle large datasets and the need for plenty of labeled malware image data. Technical challenges persist in resolving current model update requirements to confront adaptive malware methods in their current format. Future malware detection research goals to enhance performance by integrating three main advancements between transfer learning capabilities and lightweight architecture designs and real-time feedback protocols. Through the research scientists acquire the capability to build stronger defensive measures against intricate malware threats targeting computer systems.

Keywords:
Malware Detection, Hybrid Deep Learning, CNN-LSTM, Image-Based Classification, Cybersecurity.

Introduction

The total number of new malicious programmed malware kinds and versions that are available on the internet has been steadily rising. According to Kaspersky Labs most recent “Number of the year” technical report, 360 000 new malware files are discovered per day, an increase of 11.5% over the previous year. Their cloud database has over one billion unique malware files[1]. Developing defense mechanisms against malicious software (malware) attacks is essential as these attacks have the ability to take down companies by accessing their data, apps, and computer systems without the consent or authorization of the user[2]. Nowadays, malware proliferation has become a vital security concern, which is caused by the quick expansion of cyber-criminal activities[3]. Digital criminals start to explore other approaches constantly and therefore, the former signature-based identification schemes are not so precise for the newly-developed and high-level malware variant. Most seriously cybercriminals are constantly seeking additional tools to cause more crimes and are investing well in them. This challenges the cybersecurity and research professionals to introduce and apply advanced technique such as deep learning to enhance detection capabilities[4], [5].

Artificial Intelligence, which is a type of learning inspired by our brains, offers a sub component known as deep learning which has been proven to be quite effective in domains such as computer vision, NLP and speech recognition. This is because deep neural networks are nowadays being used to extract sophisticated representations from large databases for more enhanced and effective detection of malware[6]. Deep learning is viewed as a possible strategy to investigate visual attributes associated with image-based malware. Considering the fact that cyber-attackers are currently using images and image files primarily for malicious purposes with trojan zed images in particular and images with embedded payloads there is now a great demand for detection approaches that can successfully identify such threats[7], [8]. Nevertheless, deep learning models have been shown to be effective in various tasks and have particularly empowered image-based malware detection processes with some notable constraints. There are some challenges and one of them is that there are not many labeled datasets available that contain a wide range of examples of malware images that are representative[9]. The creation of such datasets can be a tedious and expensive process especially when doing so for a dynamic malware ecosystem.

Deep learning models that are currently used cannot handle new and unseen samples of malware causing threats in the real-world systems. In response, scientists have started investigating the possible integration of deep learning with other methods like transfer learning, ensemble modelling, and adversarial methods to overcome the foregoing challenges[3]. Hybrid deep learning models are designed to combine different learning methodologies to enhance the prediction efficiency and performance of deep learning models for malware detection in the real-world and real-time manner[10].Thorough review of the existing studies on hybrid deep learning strategies for image-based malware detection, continued benefits and challenges, and possible future research directions[4]. We hope to present these insights through examining the results of recent studies and experiments based on hybrid deep learning techniques for image-based malware detection methods, associated challenges, and possible solutions. The analysis of the individual hybrid models' strengths and weaknesses will help to better the design of the future hybrid models that will make it easy in developing early and more effective malware detection systems that will be able to deal with the everchanging threats to the cyber world.

Literature Review

Studies about hybrid deep learning for malware detection with an emphasis on image-based malware detection have become increasingly significant. Researchers have given intense focus to image-based malware detection approaches during the recent years. Here are some Several previous research papers together with studies demonstrated relevance to hybrid deep learning effectiveness in this domain[11], [12]. learning in this domain: A research article titled "Deep Learning Based Malware Detection using Hybrid Convolutional Neural Networks" was written by [12]. The results in the work of are based on a hybrid deep learning system for detecting malware. During its detection operations, the system applies both Convolutional Neural Networks (CNNs) and traditional machine learning classifiers. CNNs work as image-based features extractor for Malware binaries, which is provided to CNNs for image-based processing, prior to being fed into traditional ML classifiers for the classification[10]. The proof of the combined system's success at providing superior capabilities of malware identification is established in the research. With traditional ML classifiers, the detection accuracy increases when deep learning CNNs run with them instead of alone. new mixed deep learning system for malware detection [13] is centered on the use of LSTM and traditional ML algorithms. LSTM network takes a time series data produced by malwares into account. In this method, traditional ML algorithms are used for the classification duties. Results from the combined framework depict better results than the results from single models[13].Adversarial Deep Learning for Robust Detection of Binary Encoded Malware Images", investigated the use of adversarial deep learning techniques and proved that these techniques help increase the robustness of the malware detection system towards adversarial attacks[14], [15]. They create a complex deep learning system that combines generative adversarial GANs with ordinary ML classifiers in one comprehensive system for analyzing binary-encoded malware image[9]. As empirical findings show, hybrid model provides a better resistance to adversarial attacks. Adversarial deep learning techniques approach is stronger than deep learning or traditional ML methods alone in the protection against adversarial attacks[16]. The model focuses on some important regions of the input images through an attention mechanism in order to better capture important features for its classification. Further experimental results showed that this combination was superior in the regard of detection results[2]. The implementation of CNNs with attention mechanisms generates superior detection results when compared with CNNs operating without attention features. "Ensemble of Deep Learning and Machine Learning Approaches for Malware Detection" by [17] examined ensemble approaches to determine their capacity for combining deep learning and traditional ML techniques for malware detection. The researchers implemented an ensemble model which combines different deep learning networks including CNNs and LSTM[18]. with traditional ML classifiers (e.g., SVM, Random Forest). Experimental results the ensemble method achieved superior results compared to stand-alone models regarding detection accuracy according to experimental outcomes. accuracy and robustness. Multiple studies have proven the success of integrating deep learning method with traditional approaches in targeted detection tasks[10], [12]. image-based malware detection. Deep learning architectures work better when they are combined in one framework. Hybrid models improve detection capabilities through the strategic fusion of traditional machine learning approaches with existing machine learning techniques. performance, robustness against adversarial attacks, and generalization capabilities, such improvements lead to better detection reliability for malware threats.

Methodology

The procedure starts with collecting both legitimate and harmful samples followed by grayscale transformation on these samples before extracting pixel intensities HOG descriptors and LBP from them. The procedure begins by converting both malicious and benign samples into grayscale images while extracting pixel intensities and HOG descriptors and LBP from the pictures. descriptors, and LBP. A preprocessor transforms the features found in the CSV file through encoding and normalization procedures. The preprocess step includes applying labels after normalizing the variables in the feature dataset. The information source splits into three sections for test and validation and training purposes. training sets. The system uses a deep learning combination of long short-term memory (LSTM) networks with convolutional neural networks (CNN) to achieve its functionality. The combination of LSTM networks and convolutional neural networks establishes a deep learning structure that detects both temporal links and spatial characteristics. (CNN) to extract spatial features. The model needs evaluation for its performance in image-based detection tasks. The training process of malware detection utilizes accuracy together with precision and recall and F1-score among other testing metrics. recall, and F1-score.

Research Design

Our main contributions about utilizing binary-abstraction CNNs to identify malware form the essential sections of this paper. The research covers detection methods that show better performance compared to past approaches to detection. section.

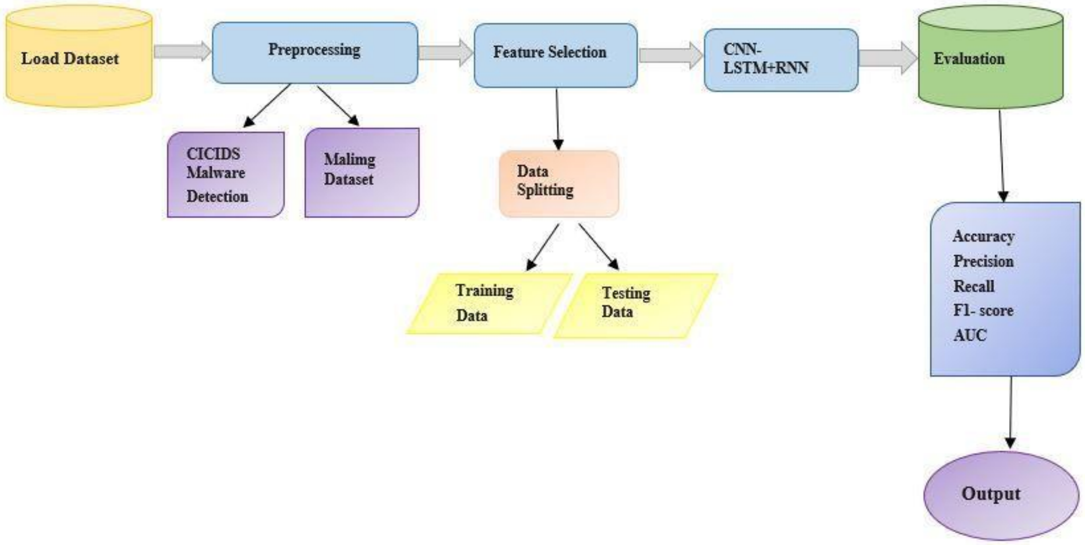

Figure 1: The Proposed Technique (CNN-LSTM+RNN)

The suggested strategies for this kind of study may include hybrid deep learning approaches and many phases. Below is a summary of the standard methodology.

1. **Binary Dataset:** The dataset arranges malware samples through binary files. In the "binary files" consist of executable files or raw data formats which make up these collections in such cases. Research scientists utilize deep learning models on files provided by the research to detect malicious activities. activities.
2. **Pre-processing:** These files is represented as a pixel when they are transformed into grayscale images.

- CCIDS Malware Dataset: A set of malicious and safe files for malware analysis.
- Malign Dataset: A dataset for deep learning analysis that includes malware families' binary representations transformed into pictures.
- Virus Share Dataset: Malware samples that can be turned into photos are include.

- MMCC Dataset: A dataset for tasks involving malware classification.

3. **Feature Stage Selection:** For "Hybrid Deep Learning Effectiveness on Image-Based Malware Detection," The dimensionality reduction, this step may entail choosing a subset of the most significant characteristics. Feature selection can reduce overfitting and enhance the model's performance. This following is the process for feature stage selection, training, and testing.

- **Splitting Data:** The preprocessed data is then divided into two sets: training data and testing data. Model is trained using training data, and evaluated on testing data on which it has never seen before. The data set is split into the training data set and the testing data set.
- **Data Retrieval:** The retrieved features are used to retrieve data from the dataset, training a hybrid model (CNN + LSTM) that attempts to find patterns (which may represent malware features).
- **Generalization:** In addition, data testing is also carried out to test the model's ability to generalize, and an independent test set containing images seen by the model only during training is considered.

Malware Image Samples

In order to detect and categorize different types of malwares, machine learning models can be trained using samples of malicious software, or malware. Executable files, photos (for image-based identification), and other elements like API calls, system activity, etc. are frequently used to represent these samples. Images produced by different malware types are included in the Maling collection. The pictures are grayscale representations of the binary bytes of malware executables (for example, using byte sequence mapping). This enables the extraction of features and patterns that can aid in categorization using CNNs (Convolutional Neural Networks).

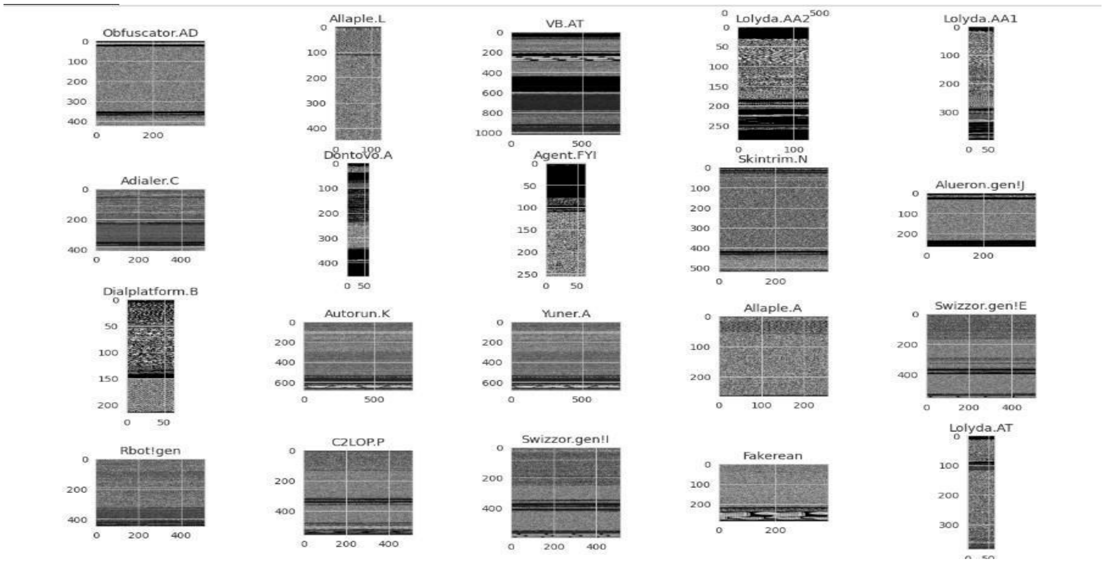

Figure 2: Malware Sample Images

Results and Discussion

In a paper Hybrid Deep Learning for Image Based Malware Detection, the authors show that Convolutional Neural Networks (CNN) and Long Short-Term Memory (LSTM) networks can detect and categorize different types of malwares in hybrid fashion with results in the order of 80 - 85% on both. The approach shows excellent accuracy as well as robustness, wherein compromised binaries are converted to the gray scale image which is then represented by CNNs and LSTMs are employed to capture the sequential dependency. Generally, performance metrics such as accuracy, precision, recall and F1 score are excellent for most malware categories. The model's capacity to generalize to novel and untested samples is improved by the utilization of the Maling dataset, which offers a varied collection of malware images. To validate the model's scalability and flexibility to changing malware threats, additional testing on separate datasets and in real-world settings is required. As new malware strains appear, maintaining the model's efficacy will require constant updates and monitoring.

Experimental Setup

Using various datasets, we experimentally investigated our suggested hybrid model. The first step in the similarity analysis was to analyze the different data mining algorithms using the Python programming language and develop distance metrics. An extensive real-life malware dataset of around 75,000 samples that were sourced from public databases like VX Heavens was used to evaluate the experiment, which was conducted in three separate processors to help with the efficient classification of malware.

The remaining samples were benign, but over two-thirds of the samples were malicious. In order to balance accuracy and computational efficiency, the Hybrid Deep Learning Model experimental setup for image-based malware detection was created. The quantity of the dataset, the complexity of the model, and the available computing power all affect how long it takes to train the model. Because of the intricacy of the CNN and LSTM designs, the training procedure usually takes a considerable amount of time for the Maling dataset, which contains a big number of malware images. On a powerful GPU system, the model may take several hours to train on average with batch sizes of 32 or 64 and training for 50-100 epochs.

Classification Metrics-Based Comparison

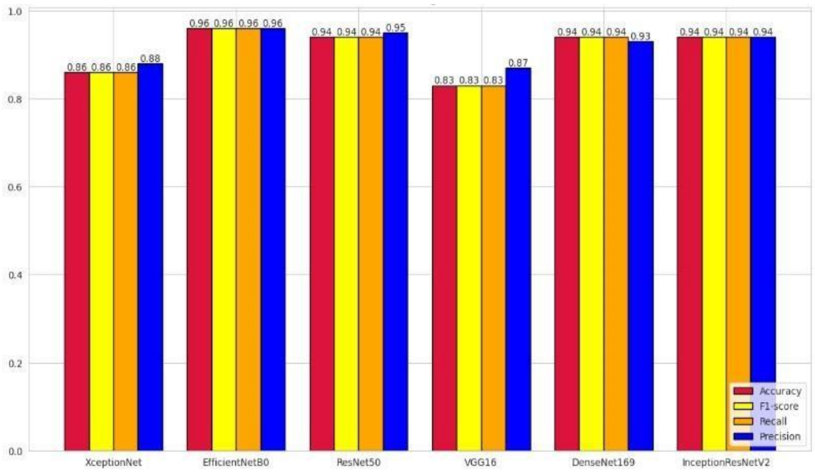

Figure 3: Classification Training History Comparison of Malign Dataset

Blended Dataset

A blended dataset is a data combined of different families of malware or a set of data from various or different types of malwares for completer and more proper dataset. They are capable of accepting multiple sources of virus, file kinds, or the combination of image contents as well as the usual feature representations. The purpose behind it is that it should increase the model's resilience of detecting malware in different domain. Given the Blended dataset could contain information from many malware families and may blend synthetic malware images with actual malware samples in some research, particularly in hybrid deep learning, particularly where the points of inflection lie. Data blending improves the model's ability to classify and identify the numerous attributes of harmful files, leading to generalization, and for detection of malware samples which might not be seen before or are highly diverse.

Classification Metrics-Based Comparison

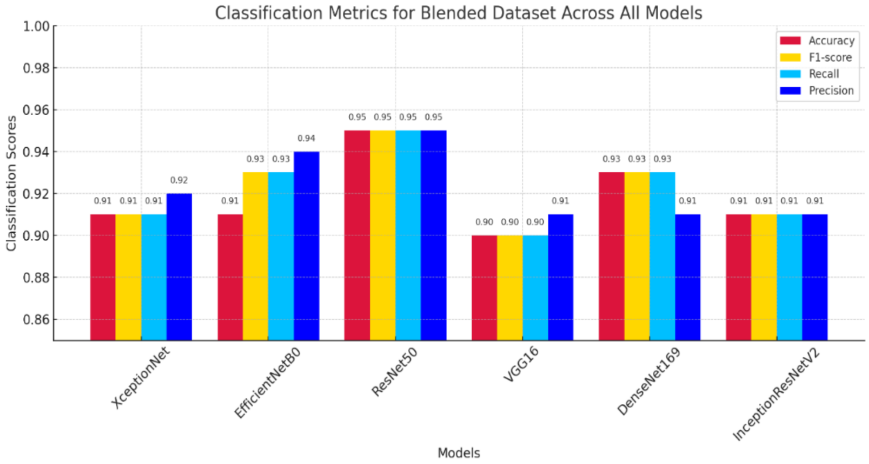

Figure 4: Classification Training Comparison of Blended Dataset

A blended dataset exists to create a strong, thorough training dataset by combining some data types (e.g. different malware representations or families). Many times, it’s used to ensure better performance, greater diversity, and better generalization in the case of malware detection tasks with machine learning models especially when using hybrid deep learning techniques.

Results of Model Training Accuracies

Table 1: Image Input Size and Accuracies on Malign and Blended

Image Input Size	Blended	Malign
48 X 48	13.50%	11.92%
64 X 64	18.92%	17.05%
128 X 128	15.01%	12.94%
224 X 224	39.46%	35.50%
360 X 360	11.29%	7.11%

F1 Scored Comparison

A model that is supposed to keep making the weights better would need more epochs always as the model attempts to learn better and do better and better accuracy and F1 score. As the CNN layers progressively learn more robust features at the malware images and the LSTM layers improve sequential modeling for classification, training the hybrid model for 50–100 epochs usually make the performance observably better.

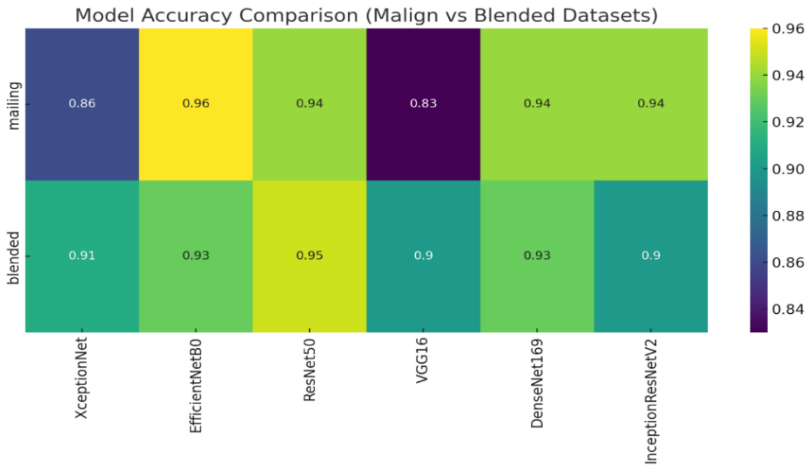

Figure 5: F1 Scored Comparison

Table 2: Mode of Training and Accuracies of Malign and Blended

Mode of Training	Blended	Malign
F1	0.94%	0.96%
Epochs	76	100
Hybrid Deep Learning (CNN-LSTM)	0.92%	0.99%

In malware detection, where classes may be unbalanced (i.e., some malware families may be underrepresented), the F1-score offers a more balanced assessment of model performance. When compared to standard machine learning models like SVM and Random Forest or single deep learning models like CNN-only, the hybrid model usually exhibits a higher F1-score. Depending on the dataset and the model's architecture quality, the hybrid deep learning model often obtains F1-scores between **0.84** and **0.96**. When compared to models with weaker recall (missing out on several malware types), the model's superior F1-score is a result of its strong generalization, even on unseen malware types.

Graph Visualization

A range of graphs and plots can be used to show the features and performance of a Hybrid Deep Learning model used for image-based malware detection. The model's accuracy, loss, and prediction time, as well as how well it performs in comparison to other models, may all be evaluated with the aid of these visualizations.

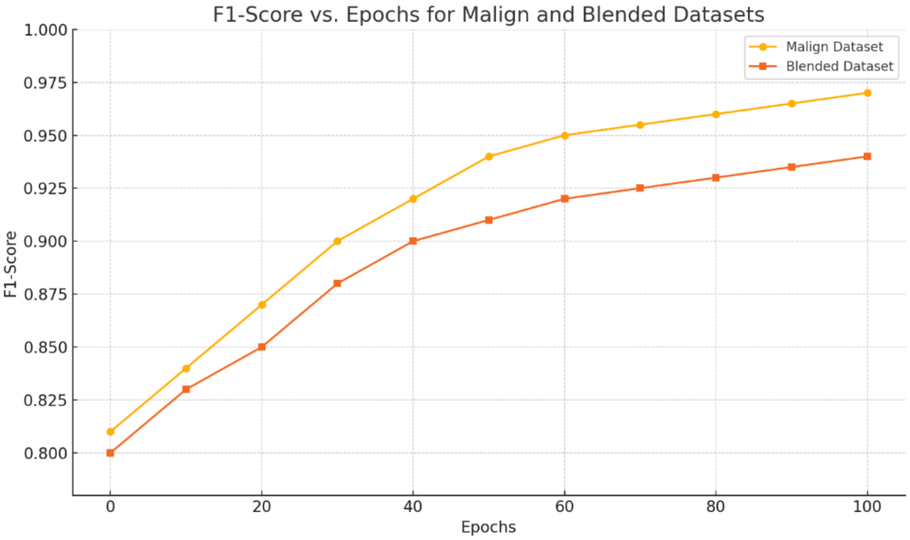

Figure 6: Graph Visualization based on F1 score

Have a better understanding of the Hybrid Deep Learning model's performance in comparison to other models by visualizing these metrics, which include classification accuracy, prediction time, and overall efficacy.

5. Conclusion

The research initializes with benchmark datasets and calculates the efficiency percentage of the proposed malware image classifies detecting model comparing with traditional CNNs and the RNNs and also evaluate of other fine-tuning approaches. The investigation shows that larger sizes are principally the prominent factors of model precision, and additional research for the perishing of input picture size on inspiration is necessary. The priority of a better crafted model pattern for certain input spaces by itself can be seen when performing a visual image of size 128 × 128 is the one that gave the maximum level of accuracy. To deal with the issue of overfitting, particularly in cases of datasets with a small number of data points, the advised way is the use of machine learning (ML), and a complex kind of convolutional neural network (CNN). The purpose of the model is to bring in more efficiency in the image classifies identification by building a new model based on the pre-trained models and then transfer learning technique. It addresses domain applicability problem by making the model capable of generalizing the input sizes of various datasets.

The visualization's provided allow to assess the performance of the model across different fine-tuning configurations. These visualization's include charts depicting accuracy and loss. It is worth noting that the highest achievable accuracies for the malign dataset are an impressive 0.96%, and for the malign dataset, an astonishing 100%. Utilizing the dense layers and final block of the pre-trained VGG-16 model for finetuning demonstrates the remarkable effectiveness of the transfer learning-based system, as indicated by these findings.

References

[1] Y. Wang, q. Wang, y. Su, b. Jing, and m. Feng, “detection of kidney bean leaf spot disease based on a hybrid deep learning model,” sci rep, vol. 15, no. 1, p. 11185, 2025.

[2] S. M. Balasubramanian, p. V. Myviliselvi, and s. Palanisamy, “implementation of malware detection using svm-based deep learning approach,” in aip conference proceedings, 2025, p. 20153.

[3] N. Aslam, m. Baqer, m. K. Abid, y. Aziz, m. Fuzail, and others, “intelligent intrusion detection for enhanced security in cloud computing,” kashf journal of multidisciplinary research, vol. 2, no. 03, pp. 22–32, 2025.

[4] A. M. Ahmad et al., “strengthening iot security with machine learning-based anomaly detection and adaptive defense mechanisms,” kashf journal of multidisciplinary research, vol. 2, no. 03, pp. 74–88, 2025.

[5] J. Ahmad et al., “utilizing deep learning techniques for detecting and analyzing food allergies,” kashf journal of multidisciplinary research, vol. 2, no. 03, pp. 46–60, 2025.

[6] S. A. Batool, m. A. Tariq, a. A. Batool, m. K. Abid, and n. Aslam, “skin cancer detection using deep learning algorithms,” journal of computing & biomedical informatics, vol. 7, no. 01, pp. 62–74, 2024.

[7] M. K. Abid, m. Qadir, s. Farid, and m. Alam, “iot environment security and privacy for smart homes,” journal of information communication technologies and robotic applications, vol. 13, no. 1, pp. 15–22, 2022.

[8] H. Nasir, a. Ayaz, s. Nizamani, s. Siraj, s. Iqbal, and m. K. Abid, “cloud computing security via intelligent intrusion detection mechanisms,” international journal of information systems and computer technologies, vol. 3, no. 1, pp. 84–92, 2024.

[9] K. R. Devi, p. S. Samyuktha, s. Bhavya, k. S. Jyothi, and r. Lakshmi, “robust intelligent malware detection using deep learning algorithms,” journal of computer science (issn no: 1549-3636), vol. 18, no. 04, 2025.

[10] Y. Song, d. Zhang, j. Wang, y. Wang, y. Wang, and p. Ding, “application of deep learning in malware detection: a review,” j big data, vol. 12, no. 1, pp. 1–29, 2025.

[11] M. Ramzan, z. U. R. Zia, m. K. Abid, n. Aslam, and m. Fuzail, “a review study on smart homes present challenges concerning awareness of security mechanism for internet of things (iot),” journal of computing & biomedical informatics, 2024.

[12] Y. A. M. Alsumaidaee, m. M. Yahya, and a. H. Yaseen, “optimizing malware detection and classification in real-time using hybrid deep learning approaches.,” international journal of safety & security engineering, vol. 15, no. 1, 2025.

[13] M. Aslam et al., “amallstm: android malware detection using lstm,” kashf journal of multidisciplinary research, vol. 2, no. 03, pp. 61–73, 2025.

[14] K. Khaliq, a. Naeem, n. Aslam, a. Malik, and k. Abid, “lccnet: a deep learning based method for the identification of lungs cancer using ct scans,” vfast transactions on software engineering, vol. 11, no. 2, pp. 80–93, 2023.

[15] N. Aslam usama tahir * muhammad kamran abid muhammad fuzail, “enhancing iot security through machine learning-driven anomaly detection,” vfast transactions on software engineering, vol. 12, no. 2, pp. 1–13, 2024.

[16] M. Ali, a. Siddique, a. Aftab, m. K. Abid, and m. Fuzail, “ai-powered customized learning paths: transforming data administration for students on digital platforms,” journal of computing & biomedical informatics, vol. 6, no. 02, pp. 195–204, 2024.

[17] H. Dong and i. Kotenko, “enhancing malware detection resilience: a u-net gan denoising framework for image-based classification.,” computers, materials & continua, vol. 82, no. 3, 2025.

[18] M. A. Tariq, w. Akbar, s. A. Batool, m. K. Abid, and n. Aslam, “breast cancer detection using deep learning algorithms,” journal of computing & biomedical informatics, 2024.