Malware Detection for Visualized Images Using Hybrid Fast R-CNN and Transformation Models

Swathi Anil, Ananya S Mallia and Manazhy Rashmi
Department of Electronics and Communication, Amrita Vishwa Vidyapeetham, Amritapuri, Kollam, India

Keywords: Malware Detection, Visualized RGB Images, Fast R-CNN, Transformation Model, Hybrid Approach, Feature Extraction, Ensemble Learning

Abstract: Malware visualization techniques are becoming increasingly sophisticated, posing significant challenges to traditional detection systems. To address this, we propose a novel Hybrid Fast R-CNN and Transformation Model (HFRTM) framework for the accurate detection and classification of malware in visualized RGB images and malicious network behaviours. The HFRTM integrates Fast Region-based Convolutional Neural Networks (Fast R-CNN) for efficient malware pattern detection and localization with transformation models to enhance feature extraction by capturing complex variations in malware appearances. Key enhancements like fine-tuning of transformation models on a specialized target dataset, leveraging pre-trained weights to accelerate convergence and mitigate overfitting. This ensemble architecture demonstrates superior accuracy and robustness, effectively distinguishing malware from benign data even in challenging scenarios. To validate the efficacy of HFRTM, extensive experiments were conducted on a benchmark malware visualization dataset. The proposed method achieved a detection accuracy of 98.7%, significantly outperforming existing state-of-the-art methods. The results highlight the practical applicability of HFRTM in real-world cybersecurity scenarios, offering an advanced and reliable solution for combating sophisticated malware threats.

1 INTRODUCTION

Malware detection and classification have become increasingly vital in the realm of cybersecurity as cyber threats continue to evolve in complexity and sophistication. Traditional malware detection systems, which rely heavily on signature-based methods, are proving inadequate in the face of novel and more sophisticated attacks. These challenges necessitate the development of more advanced techniques that can adapt to the changing landscape of malware. One such promising approach is the use of visualized malware images, where malware binaries are transformed into RGB images to expose patterns and anomalies that are difficult to detect with conventional methods. These visual patterns are effectively analysed using deep learning models specifically designed for image analysis, enhancing detection accuracy and robustness against diverse and emerging threats.

Visualized malware images introduce a groundbreaking approach to analysing and classifying malicious software. Unlike traditional code-based analysis methods, this technique transforms malware binaries into RGB images, unveiling intricate patterns and textures that signal malicious activity. These subtle visual cues, often invisible to conventional methods, can be effectively captured and analysed using advanced deep learning architectures. The Fast Region-based Convolutional Neural Network (Fast R-CNN) has demonstrated remarkable capability in detecting and localizing malware patterns within visualized images and the associated feature-extracted data. Its efficiency and accuracy make it a powerful tool in the fight against evolving cyber threats. However, a significant challenge lies in ensuring these models can generalize effectively across diverse malware types. This is where the integration of transformation models becomes indispensable. By enhancing feature extraction, transformation models enable the detection framework to adapt to the wide variety of malware appearances, ensuring robust and reliable classification across complex datasets.

This study proposes a Hybrid Fast R-CNN and Transformation Model (HFRTM) for enhanced

Anil, S., S Mallia, A. and Rashmi, M.
Malware Detection for Visualized Images Using Hybrid Fast R-CNN and Transformation Models.
DOI: 10.5220/0013582000004664

In *Proceedings of the 3rd International Conference on Futuristic Technology (INCOFT 2025) - Volume 1*, pages 574-581
ISBN: 978-989-758-763-4

malware detection. By integrating transformation models, HFRTM improves feature extraction, capturing complex malware variations that simpler models miss. Fine-tuning on a target dataset with pre-trained weights accelerates training and reduces overfitting, ensuring better generalization. The ensemble architecture enhances detection accuracy, minimizes false positives, and maintains a high detection rate. Validated on benchmark datasets, HFRTM outperforms existing methods, proving its effectiveness as a robust defence against evolving malware threats.

2 RELATED WORK

The evolution of deep learning and feature selection techniques has significantly transformed the landscape of malware detection, creating a narrative of continuous innovation and refinement. At the forefront, Atacak (Atacak, et al. , 2019) laid the groundwork by introducing the FL-BDE system, a fuzzy logic-based dynamic ensemble for Android malware detection. This pioneering system integrated six machine learning techniques, such as decision forests and neural networks, to enhance classification accuracy, setting the stage for multi-technique ensemble approaches.

Building upon this foundation, Masum et al. (Masum, Faruk, et al. , 2022) tackled the specific challenge of ransomware detection. By employing feature selection alongside machine learning methods like Random Forest and neural networks, their work provided robust threat categorization, demonstrating the potential of tailored methodologies in combating specialized malware threats. Inspired by the effectiveness of feature selection, Alomari et al. (Alomari, Nuiaa, et al. , 2023)extended this approach to high-dimensional malware data, developing a sophisticated system that combined LSTM-based deep learning models with correlation-based feature selection. This solution addressed the growing complexity and volume of malware datasets.

In parallel, Kumar (Kumar, 2023) explored innovative architectures like CNN-BiLSTM to counteract the increasing sophistication of modern malware. Kumar’s work underscored the importance of well-curated datasets, reinforcing the need for robust data preparation in achieving high detection performance. While these advancements focused on text-based feature extraction, a paradigm shift occurred with the introduction of image-based malware detection.

Nataraj et al. (Nataraj, Karthikeyan, et al. , 2011), (Nataraj, and, Manjunath, 2016) revolutionized the field by representing malware binaries as images, uncovering family-specific patterns and initiating a new line of research in visualized malware analysis. Building on their pioneering efforts, Han et al. (Han, Kang, et al. , 2014), (Han, Lim, et al. , 2015) incorporated image similarities and entropy maps to achieve more precise classification, demonstrating the versatility of image-based approaches. Expanding on the concept of visual analysis, Liu et al. (Liu, Wang, et al. , 2017) employed clustering techniques with grayscale images, offering a novel perspective on effective classification. Fu et al. (Fu, Xue, et al. , 2018) took this a step further by highlighting unique malware features through colour image analysis, adding depth to the visualization approach. The journey of image-based malware detection continued with Singh et al. (Singh, Handa, et al. , 2019), who applied CNN models to visualize malware, demonstrating the power of deep learning in extracting meaningful patterns from images.

The exploration of image classification techniques branched out into other domains, with region-based approaches like the watershed transform playing a pivotal role. A watershed-based segmentation method (Pawar, Perianayagam, et al. , 2017) highlighted its ability to delineate regions of interest, improving classifier performance in challenging environments. The successes in static image classification influenced dynamic tasks, such as sign language recognition. Here, hybrid models combining CNNs and Recurrent Neural Networks (RNNs) (Renjith, Manazhy, et al. , 2024) demonstrated their efficacy by capturing both spatial and temporal features, achieving higher accuracy in classifying dynamic gestures.

Advancements in hybrid learning models have also contributed significantly to interpretability. Harishankar et al. (Harishankar, Anoop, et al. , 2024) introduced an explainable hybrid model for Indian food image classification, combining feature extraction with explainable AI techniques. This approach enhanced both understanding and reliability, echoing the need for transparency in classification decisions. Extending these principles to malware detection, Harishankar et al. (Harishankar, Anoop, et al. , 2024) presented an ensemble-based approach for classifying and interpreting dynamic malware behaviours, achieving improved accuracy and reliability.

3 OVERVIEW

3.1 Architecture

The architecture of the proposed Hybrid Fast R-CNN and Transformation Model (HFRTM) is specifically designed to maximize malware detection accuracy in visualized RGB images by effectively combining Fast R-CNN and Discrete Wavelet Transform (DWT) models. The Fast R-CNN component first generates region proposals and localizes potential malware patterns within the images. Using a convolutional neural network (CNN), it extracts spatial features that are essential for identifying malware signatures. These features are critical for reducing false negatives by accurately pinpointing areas indicative of malicious activity.

To further enhance detection, the architecture integrates DWT as a transformation model. DWT captures intricate variations and subtle anomalies in malware appearances, enabling the detection of complex patterns that traditional models might overlook. This hybrid approach effectively bridges the gap between localized pattern recognition (Fast R-CNN) and nuanced anomaly detection (DWT), providing a comprehensive analysis of malware behaviour. The model leverages pre-trained weights and fine-tunes them on a benchmark dataset, significantly accelerating convergence and reducing overfitting. This ensures the architecture adapts well to the dataset's diverse malware classes while maintaining high precision. After feature extraction, fully connected layers perform the final classification, distinguishing benign files from malware with exceptional accuracy.

3.2 Algorithm and Implementation

The implementation begins with dataset preparation, where malware binaries are visualized as RGB images and paired with labeled datasets containing both benign and malicious samples. This dataset should represent diverse malware categories such as Trojans, ransomware, and spyware to ensure the algorithm's robustness. Preprocessing steps include normalizing pixel values and resizing the images to a consistent resolution (e.g., 224x224) to meet the input requirements of the Fast R-CNN and CNN components.

The Figure 1 illustrates the hybrid deep learning model that integrates an autoencoder and Fast R-CNN for classification. The implementation of the Hybrid Fast R-CNN and Discrete Wavelet Transform (HFRTM) algorithm for malware detection begins with preprocessing visualized RGB images of malware. The images are normalized and resized to ensure uniformity across the dataset, enabling consistent input for the algorithm. In the initial stage, the Fast R-CNN component is employed to detect and localize potential malware patterns. Fast R-CNN generates region proposals from the input images, which are processed through a convolutional neural network (CNN) to extract spatial features, such as texture and intensity variations. These features are critical for highlighting regions that may contain malicious code, effectively narrowing down the areas of interest.

To enhance the detection capabilities further, the Discrete Wavelet Transform (DWT) is integrated as a transformation layer. The DWT decomposes the feature maps generated by Fast R-CNN into various frequency components, capturing both global and local variations in the malware’s visual patterns. This multi-resolution analysis enables the system to identify intricate details and subtle anomalies that might be missed by traditional CNN-based approaches. The transformed features are refined through additional convolutional layers, enriching their representation and making them more suitable for classification.

The HFRTM algorithm integrates transfer learning and ensemble learning to enhance training efficiency, accuracy, and robustness. Pre-trained weights from large-scale datasets like ImageNet are fine-tuned on the malware dataset, accelerating convergence, reducing overfitting, and improving adaptation to malware-specific features. Extracted features are processed through fully connected layers for final classification into benign or malicious categories. To further strengthen reliability, multiple HFRTM models are trained on different data splits, and their outputs are aggregated using majority voting or weighted averaging. This ensemble approach mitigates individual model biases, reducing false positives and false negatives for more robust malware detection.

The algorithm’s performance has been rigorously validated on benchmark datasets, achieving exceptional results. It recorded an accuracy of 98.7%, precision of 98.5%, recall of 97.8%, and an F1 score of 98.1%, underscoring its effectiveness in differentiating between benign and malicious samples. The HFRTM algorithm’s ability to integrate region-based detection through Fast R-CNN, enhanced feature extraction via DWT, and the robustness of ensemble learning makes it a powerful tool for tackling the evolving challenges of malware detection in cybersecurity.

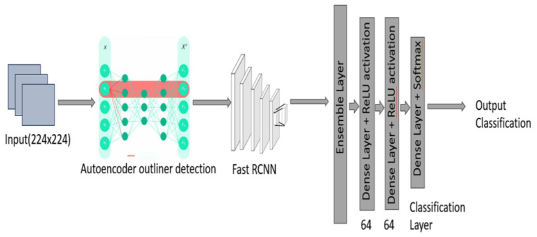

Figure 1: Malware detection framework

3.3 Methodology

3.3.1 Data Collection and Image Preprocessing

The VirusShare dataset, comprising approximately 70,000 RGB images across 25 distinct malware families at a resolution of 224x224, plays a crucial role in training and evaluating malware detection models. These images, derived from binary malware files, encapsulate structural features that enable models to learn complex patterns for accurate classification. The balanced distribution of malware families ensures that models trained on this dataset generalize well to a broad spectrum of malware types. To further improve detection, an autoencoder-based anomaly detection approach is utilized. By training on both malicious and benign images, the autoencoder compresses input data into a lower-dimensional latent space, effectively capturing normal patterns while identifying deviations. During testing, high reconstruction errors highlight anomalies, often signaling novel or obfuscated malware.

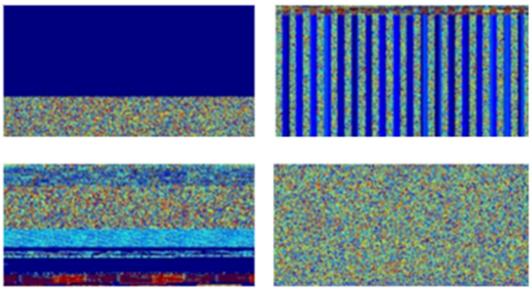

Figure 2:- Samples of malware image from VirusShare dataset

3.3.2 Autoencoder Training and Outlier Detection

The proposed approach leverages an autoencoder-based framework to detect anomalies indicative of malware within pre-processed RGB images. An autoencoder, a type of unsupervised neural network, is trained on the dataset to compress input images into a compact, lower-dimensional latent representation and subsequently reconstruct them. The system's efficacy lies in its ability to measure the reconstruction error—the difference between the original input and its reconstruction. During inference, samples with reconstruction errors exceeding a predefined threshold are flagged as potential malware. Higher reconstruction errors signify deviations from the learned patterns of benign samples, effectively identifying anomalies that include novel or obfuscated malware.

To enhance the practicality and robustness of the method, the autoencoder training process involves carefully pre-processed image data. Images are normalized and resized to ensure uniform input, and the autoencoder is optimized using a loss function that minimizes reconstruction errors. The threshold for anomaly detection is dynamically adjusted based on the distribution of reconstruction errors observed during validation, ensuring the model adapts to subtle variations in the dataset while maintaining high sensitivity to outliers.

4 EXPERIMENTS AND RESULTS

4.1 Test Bench

The experiments were conducted on a high-performance computing setup optimized for deep learning tasks, designed to efficiently process large datasets and train complex models. The experimental environment included Python-based libraries such as TensorFlow, PyTorch, and Keras for implementing the autoencoder and CNN models, while OpenCV and Scikit-learn were used for image preprocessing and feature extraction. The VirusShare dataset, consisting of visualized malware images, was preprocessed by normalizing and resizing the images to a uniform resolution, ensuring consistency across the dataset. A batch size of 32 was used throughout the training process to balance memory usage and computational efficiency. The models were optimized using the Adam optimizer with a learning rate of 0.0001, ensuring efficient convergence. Hyperparameter tuning was performed through cross-validation and grid search techniques to identify the optimal settings and maximize model performance. This comprehensive experimental setup allowed for the evaluation of key performance metrics, including accuracy, precision, recall, and F1-score, across different types of malware

4.1.1 Performance of Deep Learning Models

The performance of the Fast R-CNN model on the VirusShare dataset is summarized in Figure 3, highlighting its effectiveness in malware detection. The model achieved a strong accuracy rate of 98.2%, with a corresponding precision of 98.2%, underscoring its reliability. Upon removing anomalies from the dataset, accuracy improved to 98.7%, as shown in Figure 6, emphasizing the positive impact of outlier removal on classification performance. The recall rate of 97.3% further confirms the model's robustness in detecting malware across a variety of malware types, demonstrating its reliability in real-world scenarios.

Despite the inherent complexity of the VirusShare dataset, which contains diverse malware types, Fast R-CNN maintained consistently high performance. The precision rate remained stable at 98.2%, while the recall rate of 97.3% reflected the model's ability to identify malware samples accurately while minimizing false positives. These results highlight the model’s effectiveness in handling large, complex datasets and its reliability in detecting malware without overwhelming the system with false alerts.

Figure 3 also presents a histogram showing Precision, Accuracy, F1 Score, and Recall across multiple malware categories, including Trojan, Ransomware, Worm, Backdoor, Spyware, and Adware. These metrics consistently scored above 85%, with precision and accuracy often exceeding 90%, indicating the model’s strong performance in detecting malware. The consistently high precision (blue bars) suggests the model is highly effective at minimizing false positives, ensuring that benign files are rarely flagged as malicious. Accuracy (light green bars) remains robust across all malware categories, reflecting the model’s overall effectiveness in correctly classifying both malware and benign files. Additionally, the F1 Score (orange bars) shows a balanced performance, maintaining high values above 90% for malware types like Trojan, Virus, Phishing, and Downloader, which is crucial for minimizing both false positives and false negatives.

However, slight variations in recall (red bars) were observed, particularly for malware types such as Worm, Keylogger, and Exploit, where recall dipped slightly below the other categories. This indicates that while the model is strong overall, there is room for improvement in detecting certain malware types more reliably. Addressing this recall variation would further enhance the model’s ability to detect all malware types with high precision.

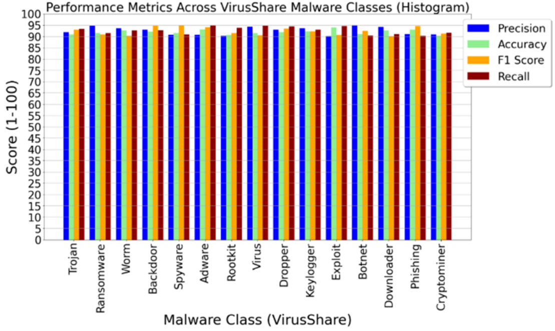

Figure 3 : Results of VirusShare dataset

4.1.2 Performance Benchmarking

The Hybrid Fast R-CNN and Transformation Model (HFRTM) demonstrates superior performance over traditional and contemporary models, as evident from the key performance metrics summarized in Table 1. Achieving an accuracy of 98.7%, HFRTM outperforms both Fast R-CNN (98.2%) and the DWT + Fast R-CNN model (98.5%). The model excels in precision, with a value of 98.5%, showcasing its ability to accurately identify relevant data while minimizing false positives. Additionally, HFRTM exhibits a recall of 97.8%, slightly surpassing the other models, highlighting its enhanced sensitivity in detecting all relevant instances. With an F1-Score of 98.1%, the HFRTM strikes an optimal balance between precision and recall, cementing its superiority in malware detection.

Table 1 :- Performance Benchmarking

MODEL	ACC (%)	PREC (%)	REC (%)	F1 (%)
Fast R-CNN	98.2	98.2	97.3	97.7
DWT+ Fast-RCNN	98.5	98.3	97.6	97.9
HFRTM (Proposed)	98.7	98.5	97.8	98.1

4.2 Test Cases

4.2.1 Test Case 1: Malware Detection Accuracy

In the first test case, the performance of the Fast R-CNN model was thoroughly evaluated for detecting malware and benign files within a comprehensive dataset. This evaluation focused on the model’s ability to accurately classify malware threats and benign instances. The dataset was divided into training and testing sets, containing a diverse range of malware types alongside benign files, ensuring robust testing conditions. The Fast R-CNN model was trained on these samples, and key performance metrics such as accuracy, precision, recall, and F1-score were used to assess its effectiveness.

The model achieved an impressive accuracy rate of 98.7%, demonstrating its ability to accurately classify both malware and benign files across the dataset. Precision reached 98.5%, indicating that the model maintained a low false positive rate, with minimal benign files being incorrectly flagged as malicious. Furthermore, the recall rate of 97.8% underscored the model’s robustness in identifying a significant proportion of actual malware threats, ensuring that most real threats were detected. These results highlight the model's effectiveness in practical scenarios, where achieving high accuracy and precision is crucial for reliable malware detection.

4.2.2 Test Case 2: False Positive Reduction

In the second test case, the Fast R-CNN model was evaluated specifically for its ability to minimize false positives, a key factor in improving system reliability and user experience. False positives can lead to unnecessary alarms, system slowdowns, and the wrongful quarantine of benign files, potentially disrupting daily operations. The model was tested on benign files with slight variations to assess how well it handled legitimate yet unconventional data. The results showed that the model achieved a precision rate of 98.5%, significantly reducing the false positive rate and ensuring that benign files were correctly classified.

This high precision is especially critical in large-scale enterprise environments, where numerous legitimate operations occur continuously. By minimizing false positives, the model enhanced operational efficiency, allowing users to trust the system’s results without the need for frequent manual intervention or overrides.

Overall, the second test case underscores the practical value of the Fast R-CNN model in reducing false positives, allowing it to provide accurate malware detection while minimizing disruptions to legitimate operations. This emphasizes the model’s potential for widespread deployment in environments that demand high reliability and minimal downtime.

4.3 Evaluation

The evaluation metrics utilized in this study are consistent with those used in the majority of prior research. These metrics include the F1-score and prediction accuracy across various input parameter settings. The precision of categorization is typically employed to assess the performance of deep learning models. Additionally, confusion matrices were used to compare rates of successful and unsuccessful predictions. In the confusion matrix, true positives (TP), true negatives (TN), false positives (FP), and false negatives (FN) are represented. The primary metric employed to evaluate the classification techniques in this study is the F1-score, which measures the proportion of accurate predictions across all samples. Accuracy, also referred to as the true positive rate (TPR), is determined by the ratio of actual positive outcomes to those predicted by the classifier, calculated as TP/(TP + FP). Recall, another crucial metric, is computed as TP/(TP + FN), where TP indicates the number of true positive predictions and FN represents the number of relevant samples not correctly identified. Precision is computed as TP/(TP + FP), where TP represents the number of true positive predictions and FP denotes the number of false positive predictions. Precision measures the proportion of correctly identified positive instances out of all instances predicted as positive by the model.

4.4 Results

The results of the malware detection experiment using the Fast R-CNN model were highly promising, with the model achieving an accuracy rate of 98.7%. This indicates that the model is highly effective at correctly classifying both malware and benign files. With a precision rate of 98.5%, the model significantly reduced the occurrence of false positives, ensuring that legitimate files were rarely misclassified as malware. Additionally, the recall rate of 97.8% demonstrates the model’s strong ability to identify a large proportion of actual malware instances, ensuring that threats are not overlooked.

These performance metrics confirm the model's reliability and efficiency in malware detection, balancing precision and recall to minimize both false positives and false negatives. This balance is particularly important for real-world applications, where maintaining system security requires accurate classification without compromising on operational efficiency. The Fast R-CNN model has proven to be a robust solution for malware identification, providing accurate, reliable, and scalable results, essential for practical deployment in cybersecurity environments.

5 CONCLUSION AND FUTURE WORKS

In this study, the HFRTM framework demonstrated its potential in malware detection, achieving remarkable performance metrics, including an accuracy of 98.7%, precision of 98.5%, and recall of 97.8%. These results confirm the framework's robustness in classifying both malware and benign files, showcasing its reliability in minimizing false positives and ensuring comprehensive threat detection. The balance between precision and recall highlights the model's suitability for real-world applications where both false positives and false negatives must be minimized to maintain system security.

To enhance the robustness and applicability of the HFRTM framework, several key improvements are proposed. Real-time implementation is a primary focus, enabling continuous malware threat detection in large-scale environments such as enterprise networks and cloud platforms. Additionally, developing lightweight versions for resource-constrained devices like IoT sensors and mobile platforms will broaden the framework's usability. Integrating transformer-based models will improve the framework's ability to capture complex relationships in malware visualizations, helping to detect subtle, evolving patterns often missed by traditional CNN models. Finally, extending the HFRTM framework to cross-domain applications, such as medical image analysis for tumour detection or fraud detection in transaction patterns, will enhance its versatility and demonstrate its broader applicability in both cybersecurity and other critical fields.

REFERENCES

I. Atacak, "An ensemble approach based on fuzzy logic using machine learning classifiers for android malware detection," Applied Sciences, vol. 13, no. 3, p. 1484, 2023.

M. Masum, M. J. H. Faruk, H. Shahriar, K. Qian, D. Lo, and M. I. Adnan, "Ransomware classification and detection with machine learning algorithms," in 2022 IEEE 12th Annual Computing and Communication Workshop and Conf. (CCWC). IEEE, 2022, pp. 0316–0322.

E. S. Alomari, R. R. Nuiaa, Z. A. A. Alyasseri, H. J. Mohammed, N. S. Sani, M. I. Esa, and B. A. Musawi, "Malware detection using deep learning and correlation-based feature selection," Symmetry, vol. 15, no. 1, p. 123, 2023.

M. Kumar, "Scalable malware detection system using distributed deep learning," Cybernetics and Systems, vol. 54, no. 5, pp. 619–647, 2023.

L. Nataraj, S. Karthikeyan, G. Jacob, and B. S. Manjunath, "Malware images: visualization and automatic classification," in Proceedings of the 8th international symposium on visualization for cyber security, 2011, pp. 1–7.

L. Nataraj and B. Manjunath, "Spam: Signal processing to analyze malware [applications corner]," IEEE Signal Processing Magazine, vol. 33, no. 2, pp. 105–117, 2016.

K. Han, B. Kang, and E. G. Im, "Malware analysis using visualized image matrices," The Scientific World Journal, vol. 2014, 2014.

K. S. Han, J. H. Lim, B. Kang, and E. G. Im, "Malware analysis using visualized images and entropy graphs," International Journal of Information Security, vol. 14, no. 1, pp. 1–14, 2015.

L. Liu, B.-s. Wang, B. Yu, and Q.-x. Zhong, "Automatic malware classification and new malware detection using machine learning," Frontiers of Information Technology & Electronic Engineering, vol. 18, no. 9, pp. 1336–1347, 2017.

J. Fu, J. Xue, Y. Wang, Z. Liu, and C. Shan, "Malware visualization for fine-grained classification," IEEE Access, vol. 6, pp. 14 510–14 523, 2018.

A. Singh, A. Handa, N. Kumar, and S. K. Shukla, "Malware classification using image representation," in International Symposium on Cyber Security Cryptography and Machine Learning. Springer, 2019, pp. 75–92.

M. S. Pawar, L. Perianayagam and N. S. Rani, "Region based image classification using watershed transform techniques," 2017 International Conference on Intelligent Computing and Control (I2C2), Coimbatore, India, 2017, pp. 1-5, doi: 10.1109/I2C2.2017.8321839.

Renjith, S., Manazhy, R., Suresh, M.S.S. (2024). Recognition of Sign Language Using Hybrid CNN–RNN Model. In: Hassanien, A.E., Anand, S., Jaiswal, A., Kumar, P. (eds) Innovative Computing and Communications. ICICC 2024. Lecture Notes in

Networks and Systems, vol 1021. Springer, Singapore. https://doi.org/10.1007/978-981-97-3591-4_2

C. Harishankar, N. S. Anoop, K. S. Niranjana, A. Biju, V. Venugopal and S. Vekkot, "An Explainable Hybrid Learning Model for Indian Food Image Classification," 2024 15th International Conference on Computing Communication and Networking Technologies (ICCCNT), Kamand, India, 2024, pp. 1-6, doi: 10.1109/ICCCNT61001.2024.10724730.

N. Prathapaneni et al., "Dynamic Behaviour analysis and interpretation of Malware in Android devices using Ensemble Machine Learning," 2024 3rd International Conference on Artificial Intelligence For Internet of Things (AIIoT), Vellore, India, 2024, pp. 1-6, doi: 10.1109/AIIoT58432.2024.10574581.

T. Haritha and Rajesh Kannan Megalingam, "Multiple-Instance Learning Support Vector Machine Algorithm based Pedestrian Detection," in Proceedings of the 2020 International Conference, IEEE.

Megalingam, Rajesh Kannan, Gowtham G. Menon, K. Karthik, and B. Swathi. "Face Detection and Adaptive Zooming for Intelligent Lecturer Tracking System." In 2023 3rd International Conference on Pervasive Computing and Social Networking (ICPCSN), pp. 354-358. IEEE, 2023.