



Using Spatial Pyramid Pooling Layer in Convolutional Neural Networks For Image-based Malware Detection

H.N.I. Albuquer*, T. Jeyamugan and S. Sobana

Department of Physical Science, Faculty of Applied Science, University of Vavuniya, Sri Lanka. .

Abstract: As computer technology rapidly advances, the prevalence of malware has surged, posing significant threats to network security and user data. Malware can infiltrate systems by spreading through the Internet, leading to data loss, fraud, and network breakdowns. Researchers are continually exploring methods to enhance malware detection. This study focuses on improving image-based malware detection by integrating the Spatial Pyramid Pooling (SPP) layer into Convolutional Neural Networks (CNNs). The primary challenge lies in classifying malware when converting binary files of various sizes into images using traditional CNN models, which struggle with varying input dimensions. The SPP layer addresses this by allowing CNNs to process images of different sizes more effectively, identifying features at multiple scales, and enhancing adaptability. In the methodology, malware binaries were converted into grayscale images and fed into a CNN with the SPP layer, generating fixed-length feature maps. The model was evaluated using accuracy, precision, recall, and F1-score metrics. Results showed that the model achieved a high detection accuracy of 96%, with strong performance across most malware classes, including Adialer.C, Agent.FYI, and Allaple.A. However, some malware types, such as Swizzor.gen!!l, showed variability in detection performance. These findings confirm that integrating the SPP layer into CNNs significantly enhances the model's ability to detect diverse malware types, improving its effectiveness in real-world scenarios. In conclusion, this research demonstrates that the SPP-enhanced CNN model offers a robust solution for malware detection, contributing to the cybersecurity field by providing a more adaptable and accurate automatic detection system. Further research could focus on refining the model for specific malware classes with lower detection rates.

Keywords: Convolutional Neural Networks, Cyber Security, Deep Learning, Image-Based Malware Detection, Spatial Pyramid Pooling