Accelerated Malware Classification
A Vision Transformer Solution

Shrey Bavishi, Shrey Modi
shreybavishi@google.com, shreymodi@uchicago.edu

NEURAL INFORMATION PROCESSING SYSTEMS

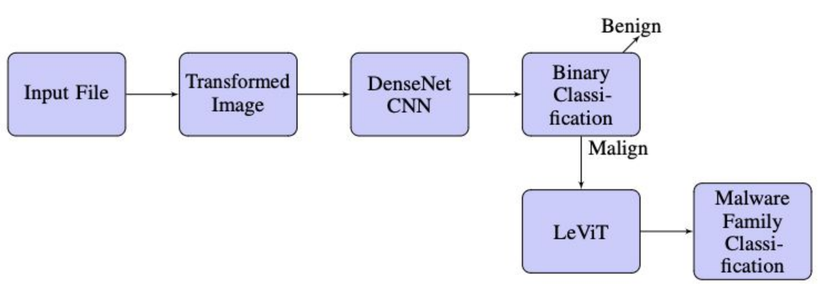
A novel architecture for fast and accurate malware classification using malware images

Introduction and Motivation

Despite industry efforts, cyber attackers continually evolve their tactics, using sophisticated evasive strategies like polymorphism, metamorphism, and code obfuscations. To address these challenges and achieve faster malware identification and classification, vision-based approaches applied to malware images have shown great promise. Our work introduces LeViT-MC, an innovative architecture that achieves state-of-the-art results in both accuracy and speed for malware classification.

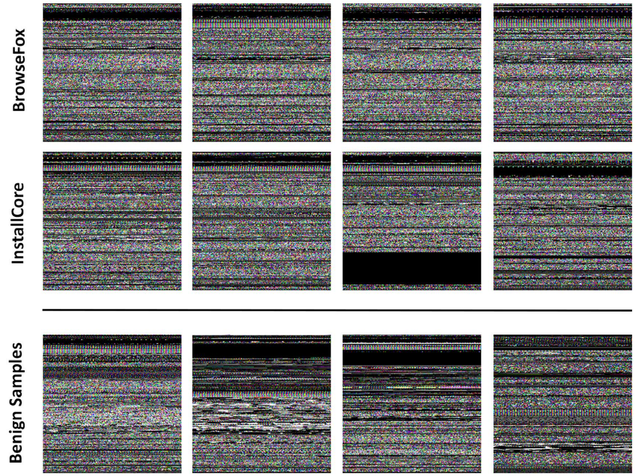
Methodology

1. Our approach involves using a 2-step approach, first for malware identification and then for classification.
2. The models are trained on malware images from the MaleVis dataset. For inference of normal files, a transformation will be required.
3. Optimal models are selected for both the tasks to increase inference speed while maintaining accuracy



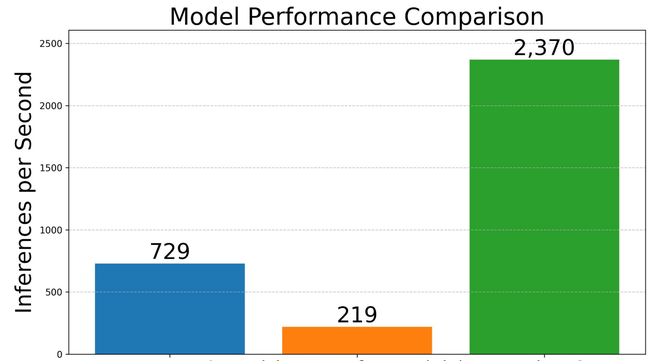
Path of a malware file

What are Malware Images? Malware images are visual representations of malicious software executables, created by transforming binary data into two-dimensional matrices that can be interpreted as images. This approach involves converting PE (Portable Executable) binary files into RGB images by reading groups of 3 bytes and arranging them in a 2D vector space



Results

- Achieved 96.6% overall accuracy in classification, outperforming previous state-of-the-art models
- Less than 1% no confusion in identification and classification
- An inference speed of 2370 images per second which also outperforms existing frameworks



Future Work

Our research demonstrates the exceptional efficacy of LeViT-MC in classifying malware images with high accuracy and minimal confusion. However, two key areas warrant further investigation:

- Performance in real-world cybersecurity infrastructures
- Investigate the underlying spatial relationships within malware binaries that enable effective CNN-based classification

References

[1] Bozkir et al. “Utilization and Comparision of Convolutional Neural Networks in Malware Recognition.” In 27th Signal Processing and Communications Applications Conference 2019

[2] Ben Graham et al “Levit: a vision transformer in convnet’s clothing for faster inference”, 2021

[3] L. Nataraj et al “Malware images: Visualization and automatic classification” In Proceedings of the 8th International Symposium on Visualization for Cyber Security, VizSec ’11