# A survey of malware detection using deep learning

**Operating System:** MacOS, Windows, iOS, Android, and Linux.

**Dataset:** standard benchmark dataset.

**Methods:** Explainable Machine Learning (XAI) or Interpretable Machine Learning (IML)

Comparative performance summary of Transfer Learning models for malware image classification:

| Model | Files | Accuracy | Dataset |
|---|---|---|---|
| CapsNet | PE | 98.63% | Malimg |
| RCNF | PE | 98.72% | Malimg |
| ResNeXt | PE | 98.32% | Malimg |
| Inception V3 | PE | 99.24% | Malimg |
| VGG16 | PE | 99.97% | Malimg |
| DenseNet | PE | 98.23% | Malimg |
| DenseNet | PE | 98.46% | BIG 2015 |
| Xception | PE | 99.03% | Malimg |
| Xception | PE | 99.17% | BIG 2015 |

Fine-tuned pre-trained models applied on different malware image datasets:

| Setting | | | |
|---|---|---|---|
| Pre-trained model | Samples | Resize image | Epoch |
| EffNet B0 | 30,000 | 224 | 200 |
| EffNet B1 | 30,000 | 240 | 200 |
| EffNet B2 | 20,000 | 260 | 200 |
| EffNet B3 | 15,000 | 300 | 400 |
| EffNet B4 | 20,000 | 380 | 400 |
| EffNet B5 | 25,000 | 456 | 400 |
| EffNet B6 | 40,000 | 528 | 400 |
| EffNet B7 | 30,000 | 600 | 1000 |
| Inception V4 | 20,000 | 229 | 300 |
| Xception | 20,000 | 229 | 200 |
| CapsNet | 3000 | 256 | 100 |

| Average accuracy | | | Our dataset |
|---|---|---|---|
| Malimg | Microsoft challenge | Drebin | Accuracy |
| 92.72% | 90.45% | 87.23% | 94.59% |
| 95.64% | 93.65% | 88.91% | 95.89% |
| 93.84% | 91.78% | 86.82% | 94.12% |
| 90.32% | 94.19% | 89.35% | 95.73% |
| 95.63% | 96.68% | 90.59% | 97.98% |
| 80.19% | 87.54% | 84.23% | 94.68% |
| 85.67% | 83.82% | 85.43% | 93.54% |
| 82.76% | 80.76% | 90.57% | 88.45% |
| 95.98% | 93.21% | 88.93% | 96.39% |
| 89.50% | 90.84% | 84.39% | 93.53% |
| 88.64% | 72.69% | 78.68% | 92.65% |

State-of-the-art deep learning models:

| Deep learning approach | OS | Features | Accuracy |
|---|---|---|---|
| MAPAS | Android | API call graphs | 91.27% |
| MaMaDroid | Android | API calls | 84.99% |
| Deep Generative Model | Android | Dalvik code, API call, Malware images, developers' signature | 97.47% |
| DeepWare | Windows/ Linux | HPC | 96.8% |
| Multi-Modal Deep Learning | Windows | Grayscale image, Byte/Entropy Histogram | 97.01% |
| Deep multi-task learning | Windows Android Linux MacOS | Grayscale color image | 99.97% |