Rajshahl University of Engineering & Technology
Department of Computer Science & Engineering

Title: Vision Based Malware Classification Framework Based On Neural Network

Supervised By

Prof. Dr. Md. Ali Hossain
Professor
Dept. Of CSE, RUET

Presented By

Shah Ahmed Saad Rupai
Roll No.: 1703069
Dept. Of CSE, RUET

19.08.2023

Table of contents

Introduction

Malware, or malicious software, refers to any type of program or code designed to harm computer systems or steal data.

There are a varieties of malwares present today , some of which are - Zeus, My-doom, Storm-worm, Slammer etc.

Different approaches have been used to detect & classify malwares. But malwares have emerged in such an extraordinary way that the traditional approaches are now not very effective.

Motivation

Traditional **signature-based** methods are less effective

A **vision-based** malware classification framework will work well

Neural Network has emerged as a promising solution

Objectives

01

develop a vision-based approach

02

develop optimized model

03

explore and evaluate models

Literature review

Paper Title & Author	Dataset & Models Used	Accuracy
Malware Images: Visualization and Automatic Classification. [1] L. Nataraj (2011)	• Malware binaries are visualized as gray-scale images • Classified using standard image features **(PCA)** and **knn** model by 10 fold cross validation using k=3	**Accuracy - 98%**
Using convolutional neural networks for classification of malware represented as images. [2] Daniel Gibert (2018)	• Malimg dataset & Microsoft Big dataset • Convolution neural network(**CNN**) is used to classify	**Accuracy: Malimg dataset - 96% & Microsoft Big dataset - 97.3%**
Towards Building an Intelligent Anti-Malware System: A Deep Learning Approach using Support Vector Machine (SVM) for Malware Classification.[3] Abien Fred M. Agarap (2019)	• Malimg dataset • **CNN-SVM**, **GRU-SVM**, and **MLP-SVM** models used for classification	**Accuracy: 84.92%**

Dataset Description

The deep learning (DL) model in this study will be evaluated on the Malimg dataset[4],

- The dataset contains 9,339 malware samples
- These malware samples are from 25 different malware families

Dataset Description Cont.

Table 1 shows the frequency distribution of malware families and their variants in the Malimg dataset[4].

No.	Family	Family Name	No. of Variants
01	Dialer	Adialer.C	122
02	Backdoor	Agent.FYI	116
03	Worm	Allaple.A	2949
04	Worm	Allaple.L	1591
05	Trojan	Alueron.gen!J	198
06	Worm:AutoIT	Autorun.K	106
07	Trojan	C2Lop.P	146
08	Trojan	C2Lop.gen!G	200
09	Dialer	Dialplatform.B	177
10	Trojan Downloader	Dontovo.A	162
11	Rogue	Fakerean	381
12	Dialer	Instantaccess	431
13	PWS	Lolyda.AA 1	213
14	PWS	Lolyda.AA 2	184
15	PWS	Lolyda.AA 3	123
16	PWS	Lolyda.AT	159
17	Trojan	Malex.gen!J	136
18	Trojan Downloader	Obfuscator.AD	142
19	Backdoor	Rbot!gen	158
20	Trojan	Skintrim.N	80
21	Trojan Downloader	Swizzor.gen!E	128
22	Trojan Downloader	Swizzor.gen!I	132
23	Worm	VB.AT	408
24	Trojan Downloader	Wintrim.BX	97
25	Worm	Yuner.A	800

Table 1: Malware families found in the Malimg Dataset[4].

Dataset Description Cont.

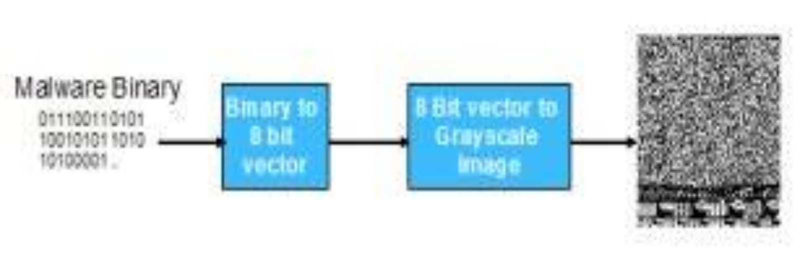

Figure 1: Image from [4]. Visualizing malware as a grayscale image.

Proposed Method

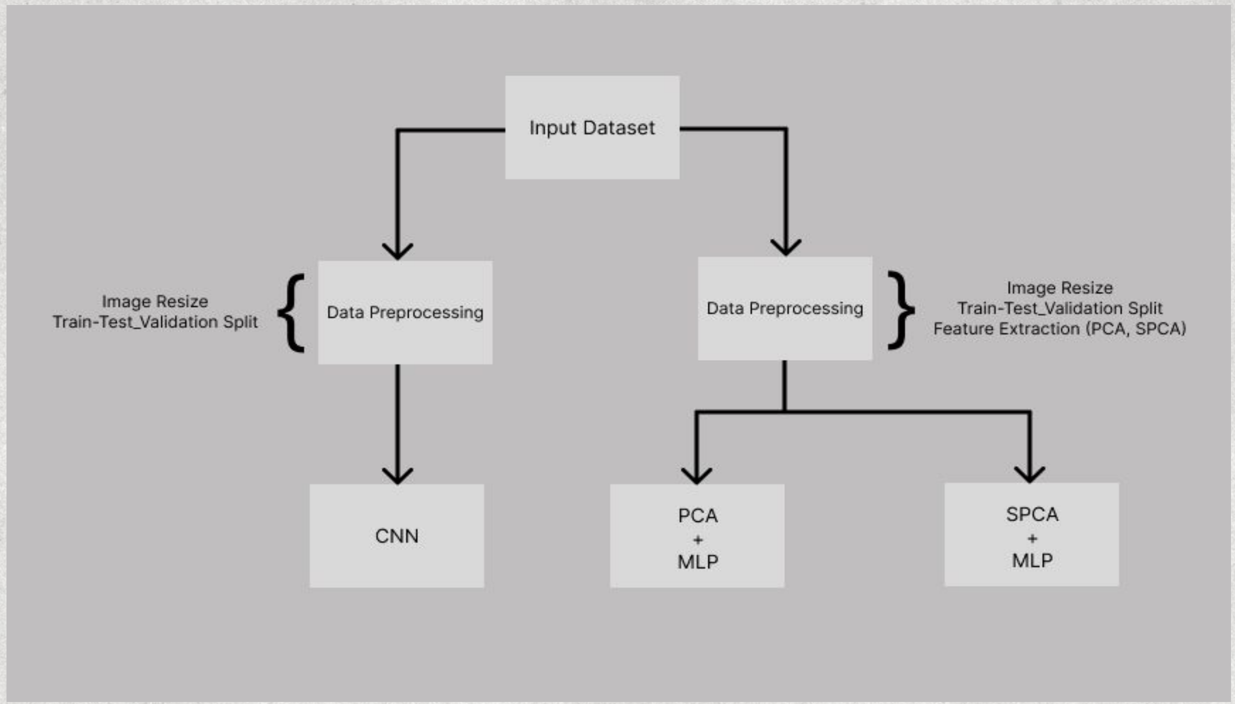

Figure 2: Workflow of the proposed method

Proposed Method Cont.

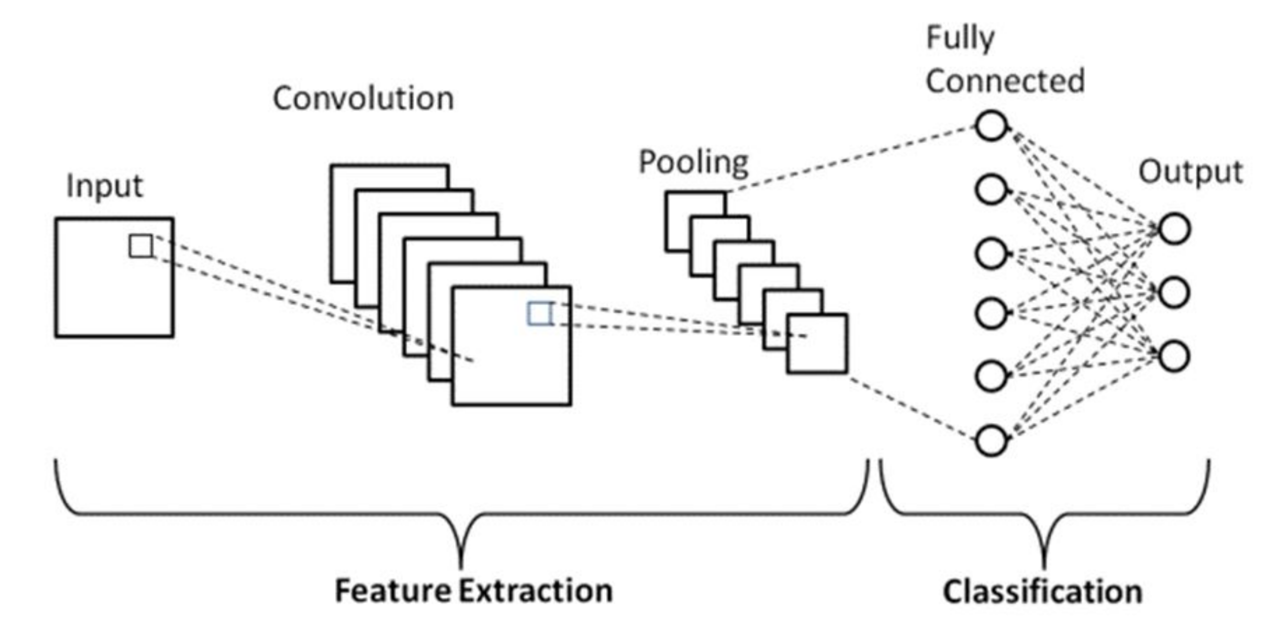

Figure 3 : Basic CNN architecture

Proposed Method Cont.

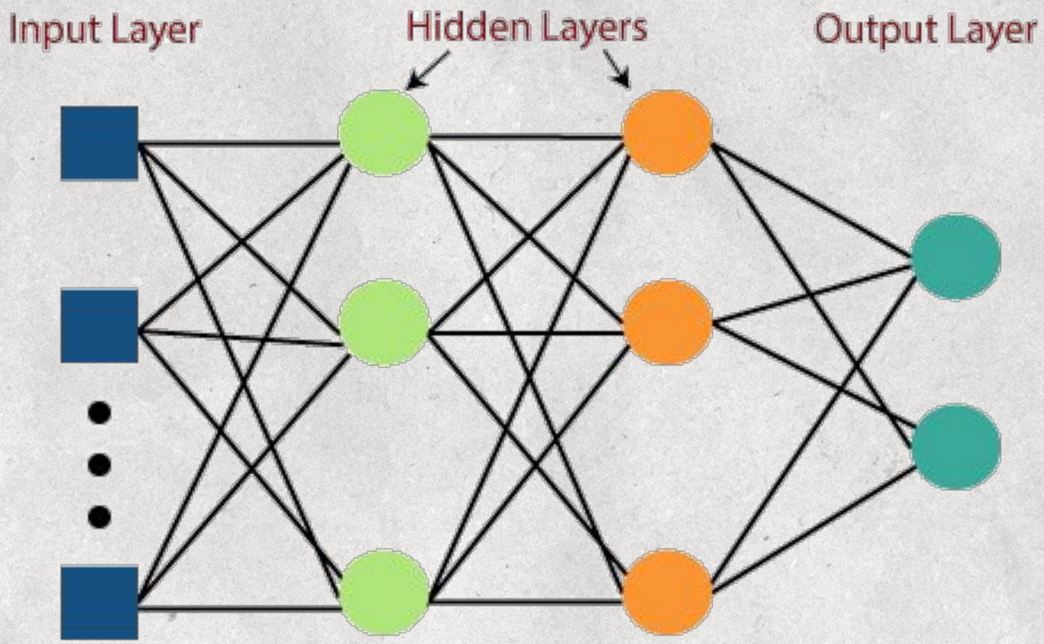

Figure 4 : Basic MLP architecture

Workflow

01

Gathering and preprocessing of data

02

Applying different model architectures

03

Analyzing the results through performance metrics like Accuracy, Precision, and F1 Score

Implementation

- Gathered Dataset and done sampling and scaling
- Converted malware binaries into grayscale image
- Applied CNN for classification
- Applied PCA and SPCA for dimensionality reduction
- Applied Multi Layer Perceptron for classification

Implementation Cont.

Figure 5 : Grayscale images of malware binaries

Result Analysis (CNN)

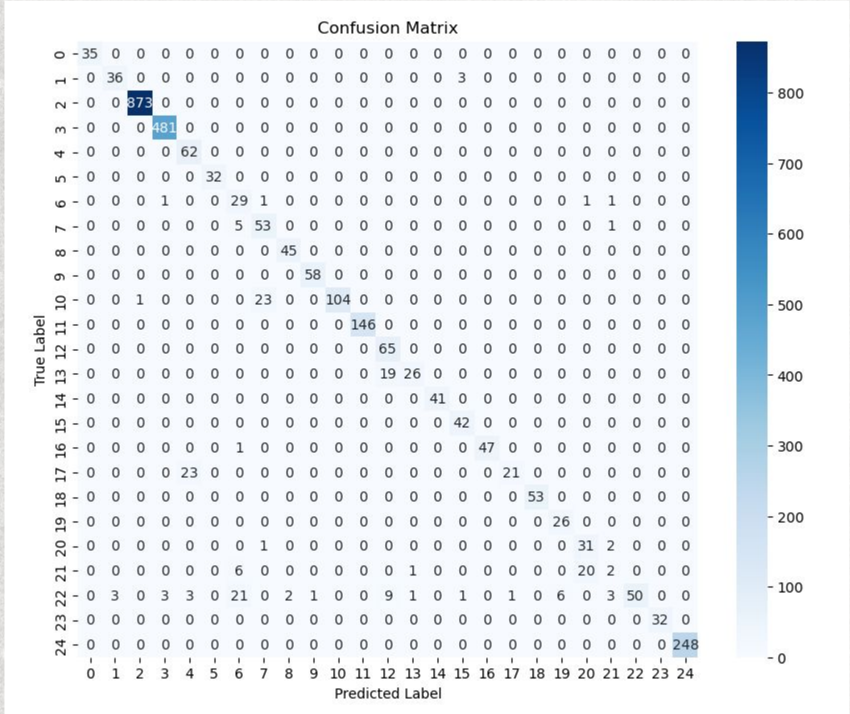

Figure 6 : Confusion Matrix using CNN model

Accuracy : 97.57%

Precision : 95.68%

F1 Score : 95.68%

Result Analysis (PCA-MLP)

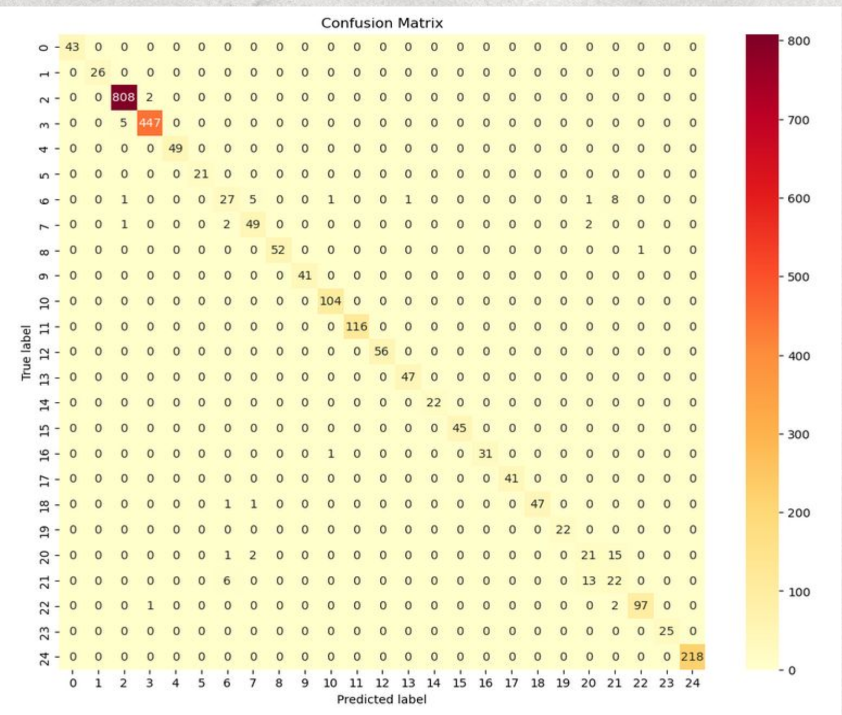

Figure 7 : Confusion Matrix using PCA-MLP model

- Components: 30
- Accuracy : 97.13%
- Precision : 94.23%
- F1 Score : 94.00%

Result Analysis (PCA-MLP)

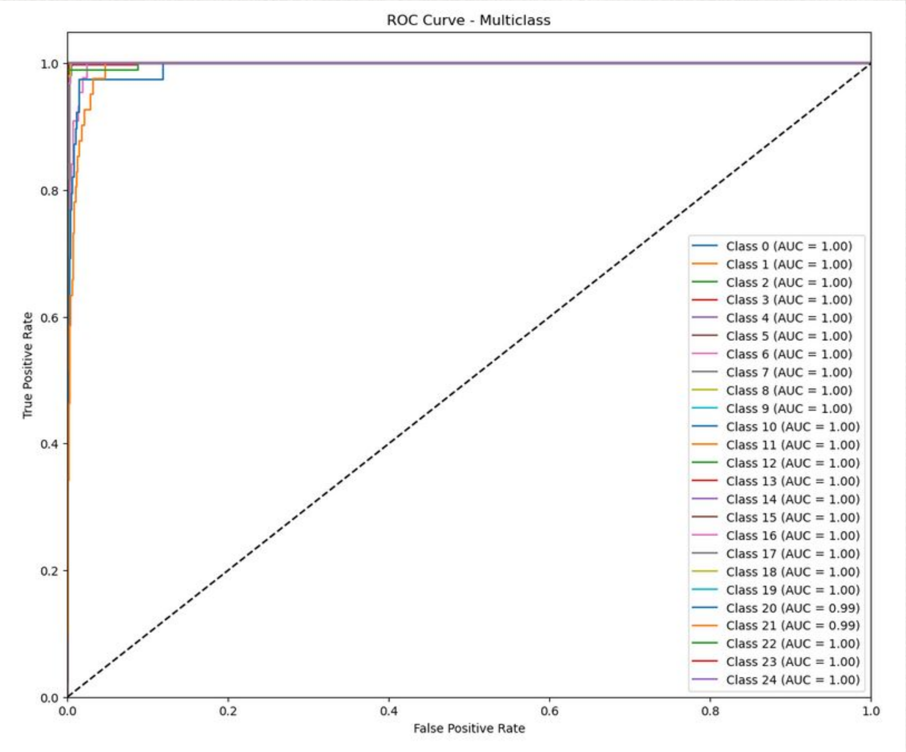

Figure 8 : ROC Curve for PCA-MLP model

- Components: 30
- Accuracy : 97.13%
- Precision : 94.23%
- F1 Score : 94.00%

Result Analysis (SPCA-MLP)

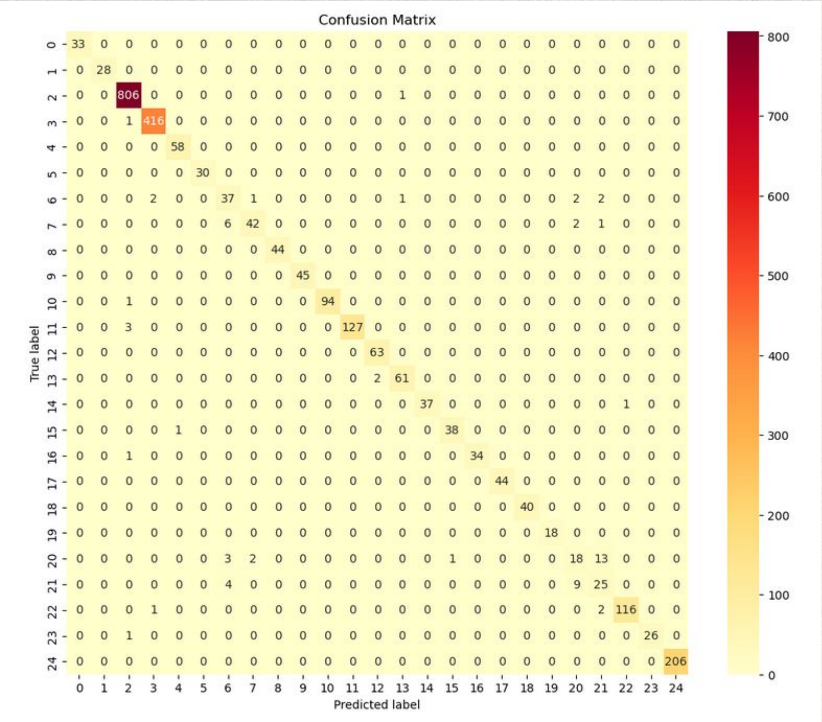

Figure 9 : Confusion Matrix using SPCA-MLP model

- Components: 30
- Accuracy : 97.49%
- Precision : 94.82%
- F1 Score : 94.51%

Result Analysis (SPCA-MLP)

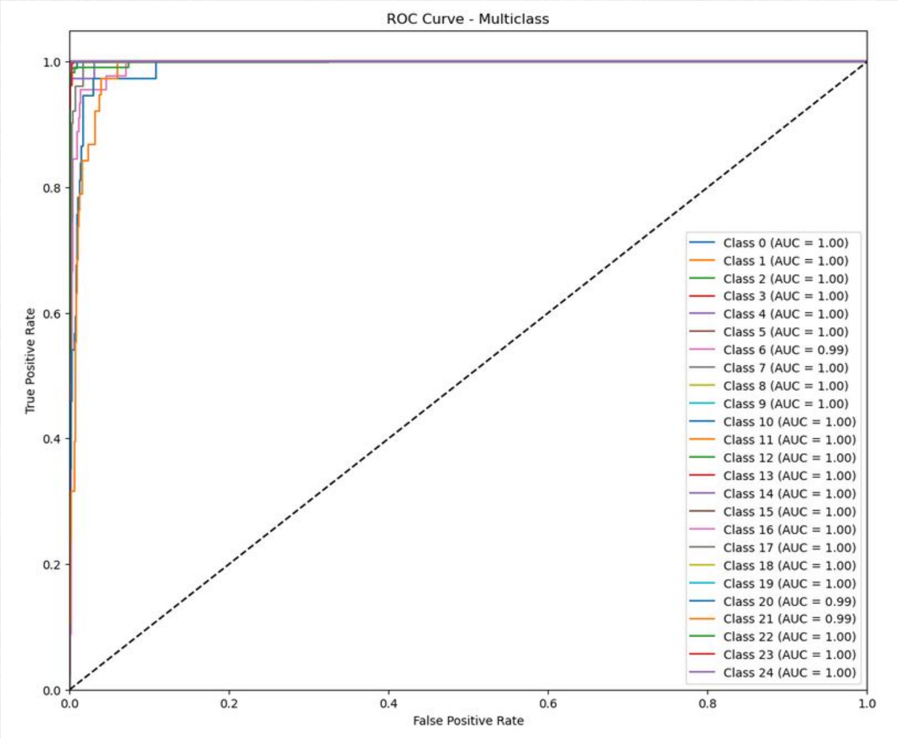

Figure 10 : Confusion Matrix using SPCA-MLP model

- Components: 30
- Accuracy : 97.49%
- Precision : 94.82%
- F1 Score : 94.51%

Model Comparison

Model	Accuracy	Recall	Precision	F1 Score
CNN	97.57%	95.68%	95.68%	95.68%
PCA-MLP	97.13%	94.69%	94.23%	94.00%
SPCA-MLP	97.49%	95.44%	94.82%	94.51%

Table 2: Comparison of the models

Future Work

Implement ResNet-152 architecture for feature extraction

Implement other deep learning models

Search for better accuracy and compare the outcomes

Conclusion

1. Vision-based malware detection can detect malware that has been encrypted to avoid detection by traditional methods

2. Vision-based malware detection can be used to detect new and unknown malware that has not yet been categorized or identified by traditional methods

3. Deep learning approach performs better than traditional methods providing better accuracy and efficiency.

Reference

[1] Nataraj, L., Karthikeyan, S., Jacob, G., Manjunath, B.S.: Malware images: visualization and automatic classification. In: Proceedings of the 8th International Symposium on Visualization for Cyber Security, VizSec '11, pp. 4:1–4:7. ACM, New York, NY, USA (2011).

[2] Gibert, D., Mateu, C., Planes, J. *et al.* Using convolutional neural networks for classification of malware represented as images. *J Comput Virol Hack Tech* **15**, 15–28 (2019).

[3] Agarap, A. F. (2017). Towards building an intelligent anti-malware system: a deep learning approach using support vector machine (SVM) for malware classification. *ArXiv Preprint ArXiv:1801.00318*.

[4] https://www.dropbox.com/s/ep8qjakfwh1rzk4/malimg_dataset.zip?dl=0

Thanks!

Do you have any questions?

saadrupai1997@gmail.com