Malware Classification using CNN and other methods comparison

R11921A16何秉學、R11921094劉宗翰、R11725007陳廷威

CONTENTS

研究及分析目的

- The number of malware attacks is rising again in 2022[1]
- Over 270,000 new **malware variants** were detected in H1 2022[1]
  - Among them, the number of ransomware accounts for a large proportion[2]
- How to detect the new variants and correctly classify their families have become an important issue
  - Understanding the families of variants help us to know the purpose of them and thus implement proper precautions to our devices

[1]Malware Statistics in 2022: Frequency, impact, cost & more (comparitech.com)
[2]Fortinet 公布《2022 上半年全球資安威脅報告》變種勒索病毒翻倍、端點設備仍是重點攻擊目標 | Meet創業小聚 (bnext.com.tw)

研究及分析目的

- In 2015, Microsoft Malware Classification Challenge[1]
  - A challenge held by Microsoft to compete with the performance of classifying Malware
- Extract features from two views and classify them with ML classification models[2]
  - hex、assembly
- DL approach has become popular recently
  - CNN based
  - Represent malware samples as images

[1][1802.10135] Microsoft Malware Classification Challenge (arxiv.org)
[2]Novel Feature Extraction, Selection and Fusion for Effective Malware Family Classification

研究及分析目的

- There are already lots of research concerning Microsoft Malware Classification Challenge
- We want to find out whether those models still perform well on different malware dataset
- **Objective:**
  Select 3 kinds of models concerning Microsoft Malware dataset and test them with Malimg dataset. Then we compare the classification results with the research results concerning Malimg dataset.

資料來源

- **Malimg**
  - 9339 malware images
  - 25 malware families

Type	Family
Worm	Allaple.A、Allaple.L、Alueron.gen!J、Autorun.K、VB.AT、Yuner.A
Trojan Downloader	Dontovo.A、Obfuscator.AD、Swizzor.gen!E、Swizzor.gen!I、Wintrim.BX
Trojan	C2LOP.P、C2LOP.gen!g、Malex.gen!J、Skintrim.N、
PWS	Lolyda.AA1、Lolyda.AA2、Lolyda.AA3、Lolyda.AT
Dialer	Adialer.C、Dialplatform.B、Instantaccess
Backdoor	Agent.FYI、Rbot!gen
Rogue	Fakerean

Malimg

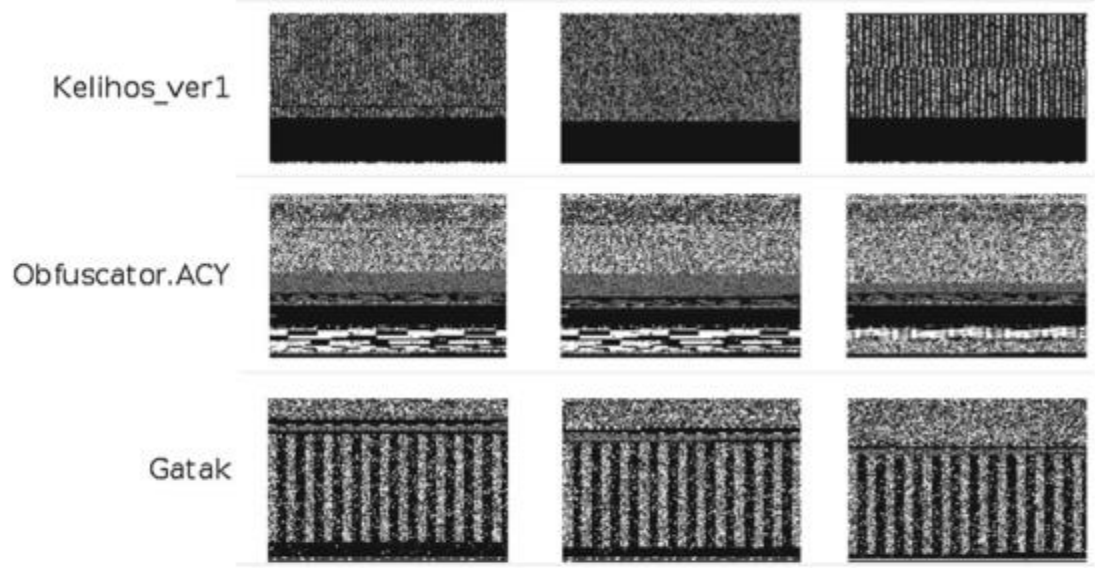


Fig. 1 Gray scale images of malicious software belonging to various families. Note that the images of malware belonging to the same family are similar while distinct from the images of malware from the rest of families

使用的工具

- Python、Tensorflow

分析過程與結果

1. Reproduce models in papers[2-4].
2. Retrain those three models based on new malware dataset - Malimg[5], see the performance of each model

TABLE I
QUANTITATIVE RESULTS ON MALIMG DATASET.

Method	Accuracy
Nataraj et al. [5]	97.18%
GIST+SVM (ours)	93.23%
M-CNN (ours)	**98.52%**

▲From[1]

[1]Kalash, M., Rochan, M., Mohammed, N., Bruce, N. D., Wang, Y., & Iqbal, F. (2018, February). Malware classification with deep convolutional neural networks. In 2018 9th IFIP international conference on new technologies, mobility and security (NTMS) (pp. 1-5). IEEE.
[2]Gibert, D., Mateu, C., Planes, J., & Vicens, R. (2018, April). Classification of malware by using structural entropy on convolutional neural networks. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 32, No. 1).
[3]Gibert, D., Mateu, C., Planes, J., & Vicens, R. (2019). Using convolutional neural networks for classification of malware represented as images. Journal of Computer Virology and Hacking Techniques, 15(1), 15-28.
[4]Quan Le a, *, Oisín Boydell a, Brian Mac Namee a, Mark Scanlon (2018). Deep learning at the shallow end: Malware classification for non-domain experts. DFRWS2018 USA - Proceedings of the Eighteenth Annual DFRWS USA
[5]L. Nataraj, S. Karthikeyan, G. Jacob, and B. Manjunath, “Malware images: visualization and automatic classification,” in Proceedings of the 8th international symposium on visualization for cyber security. ACM, 2011, p. 4.

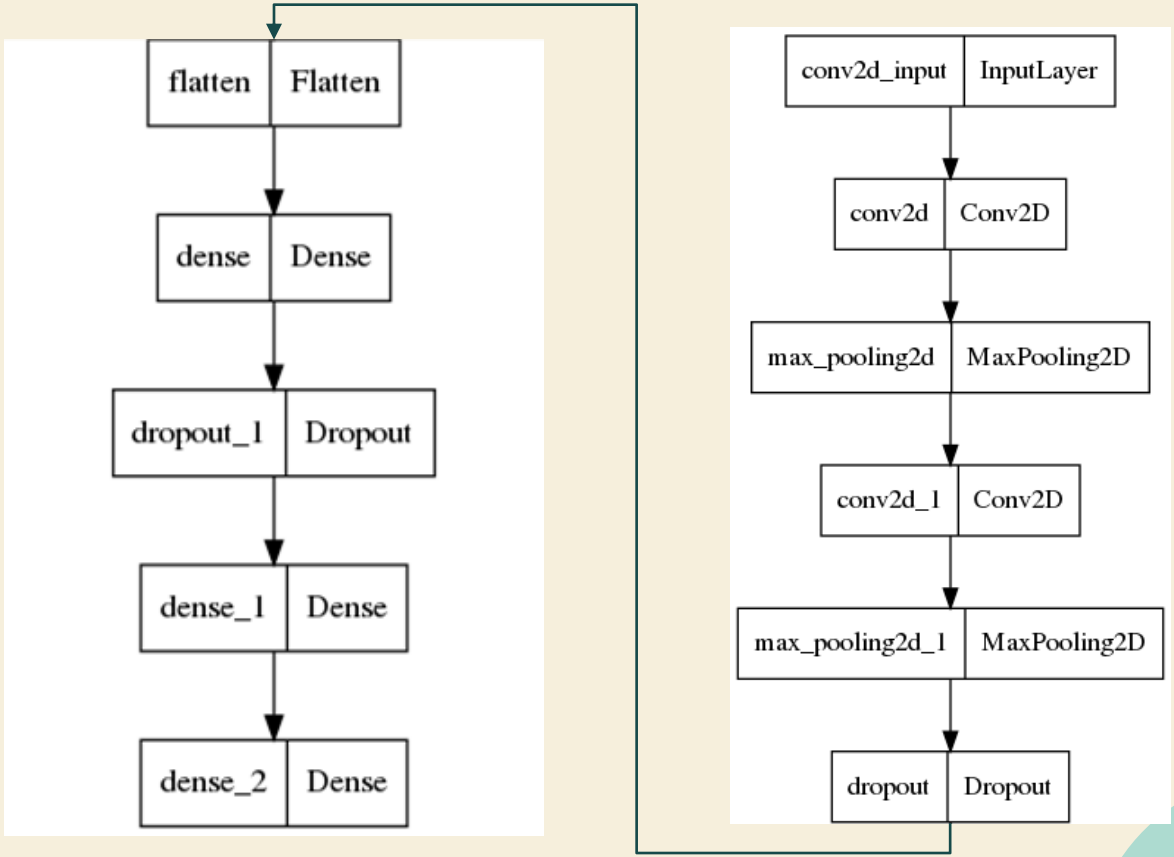
Using convolutional neural networks for classification of malware represented as images

		Accuracy (10-fold)	LogLoss	Macro F1 (10-fold)	Accuracy (5-fold)	F1 score (5-fold)			
15	**Gray-scale IMG CNN**	0.9750	0.184483	0.9400	0.973		Using Convolutional Neural Networks for Classification of Malware represented as Images		2018

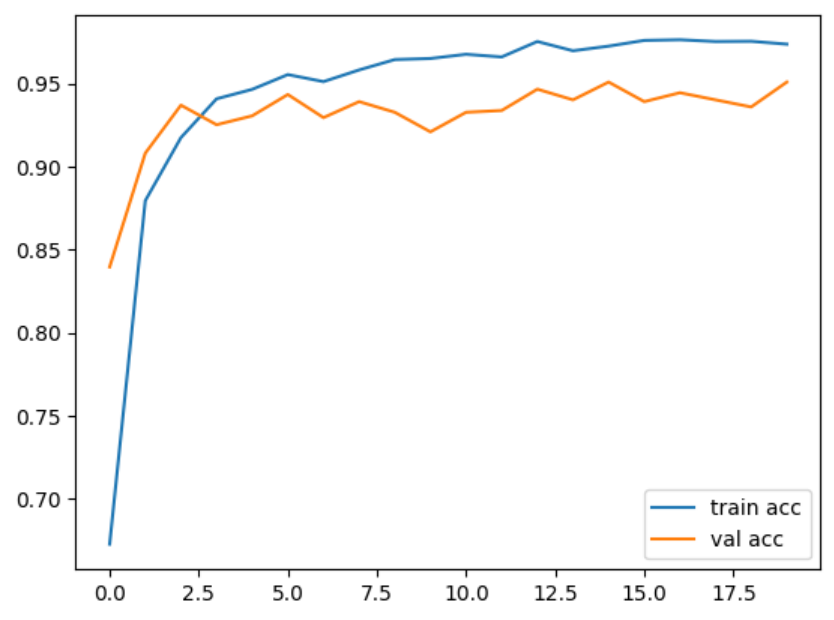
CNN-Model Configuration

- Split dataset
  - Training : 7564
  - Validation : 935
  - Test : 840
- Batch size
  - 32
- Epochs
  - 20
- Input img size
  - 150x150

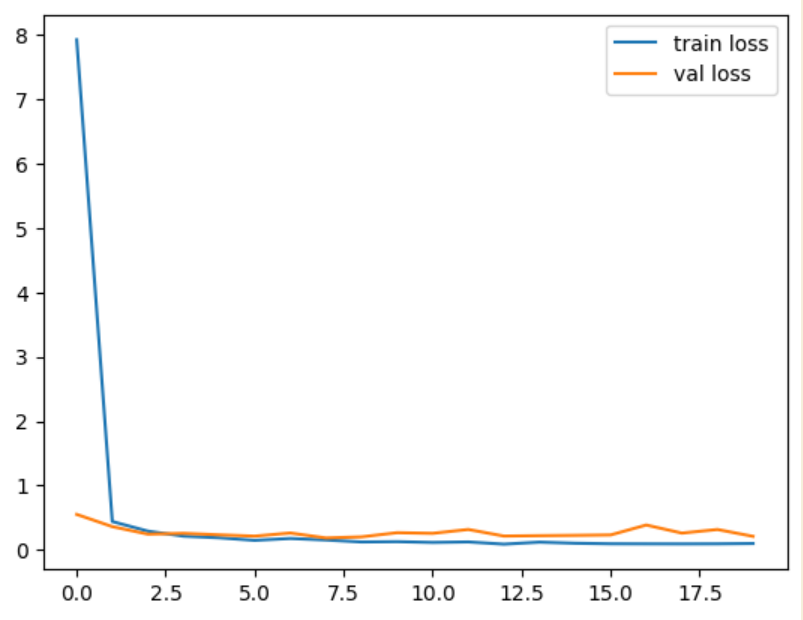
CNN-Model Configuration



CNN-Training Process



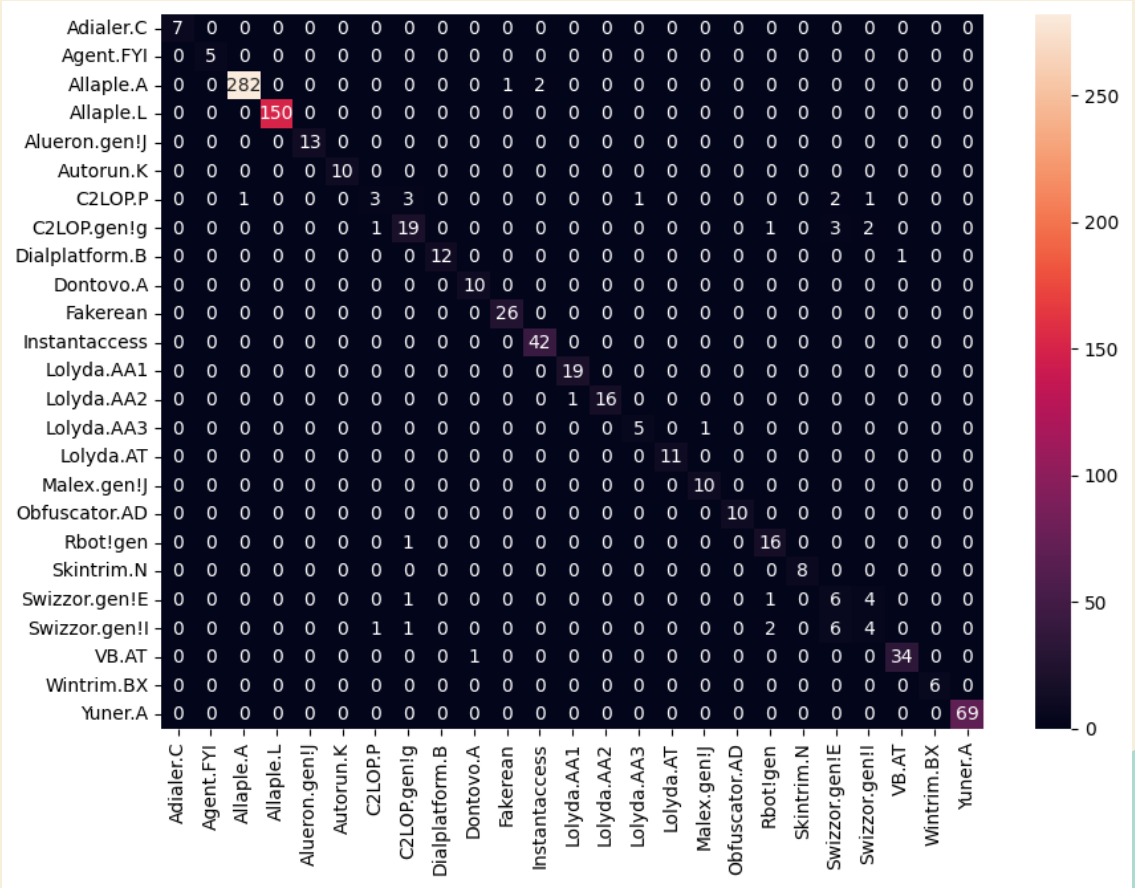
Accuracy



Loss

CNN-Results

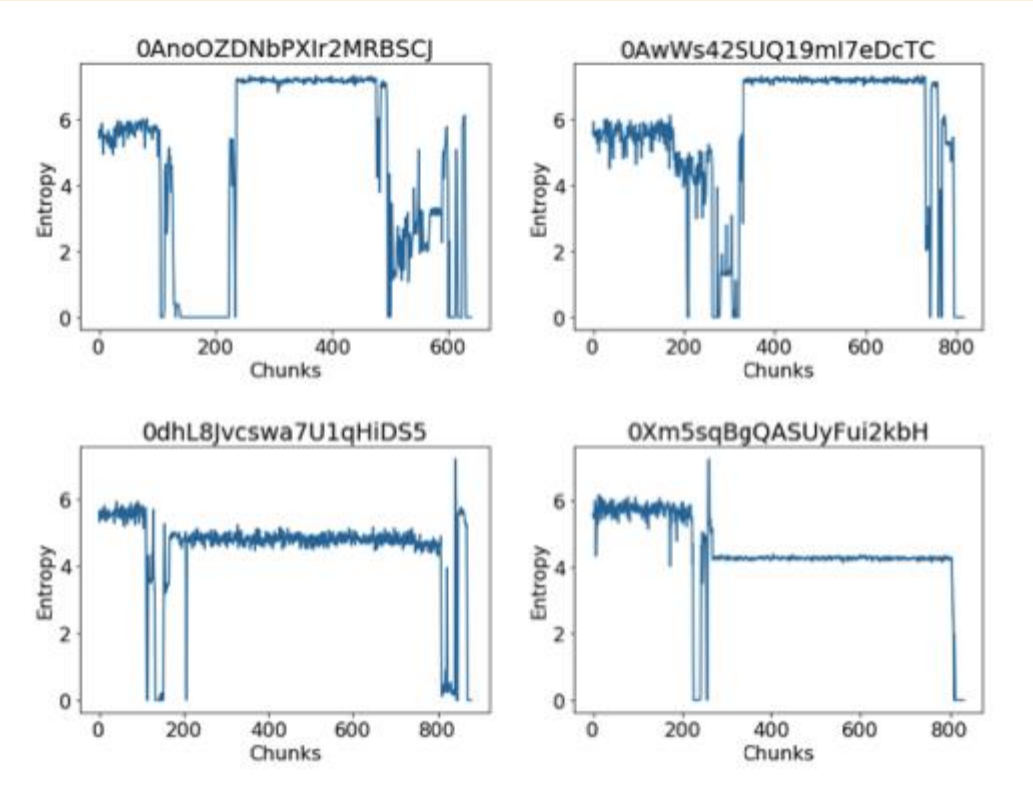
Test on 832 malware images
Accuracy: 95.31%



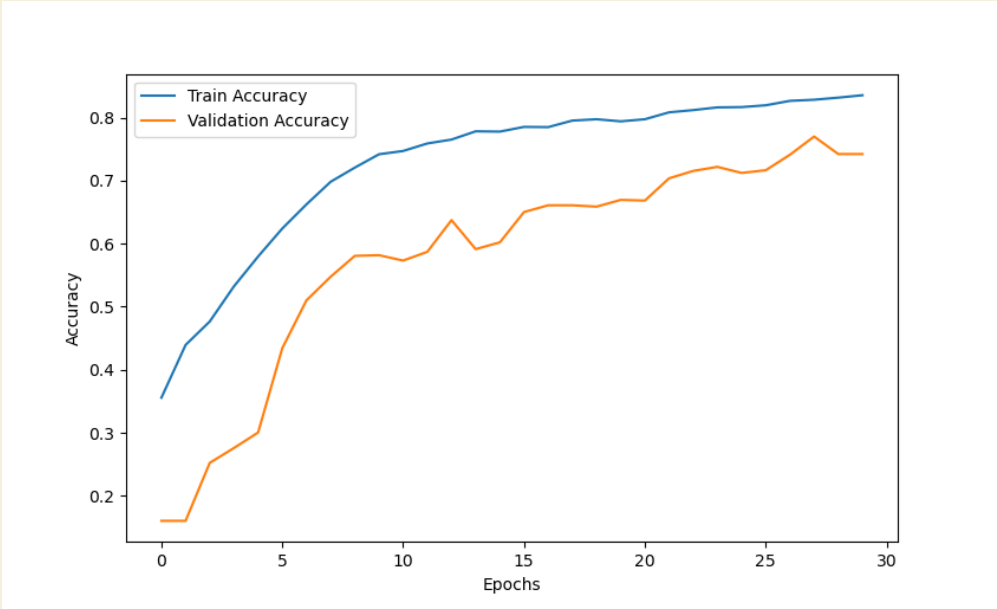
Classification of malware by using structural entropy on convolutional neural networks

		Accuracy (10-fold)	LogLoss	Macro F1 (10-fold)	Accuracy (5-fold)	F1 score (5-fold)			
17	**Structural entropy CNN**	0.9708	0.134624	0.9314			Classification of Malware by Using Structural Entropy on Convolutional Neural Networks		2018

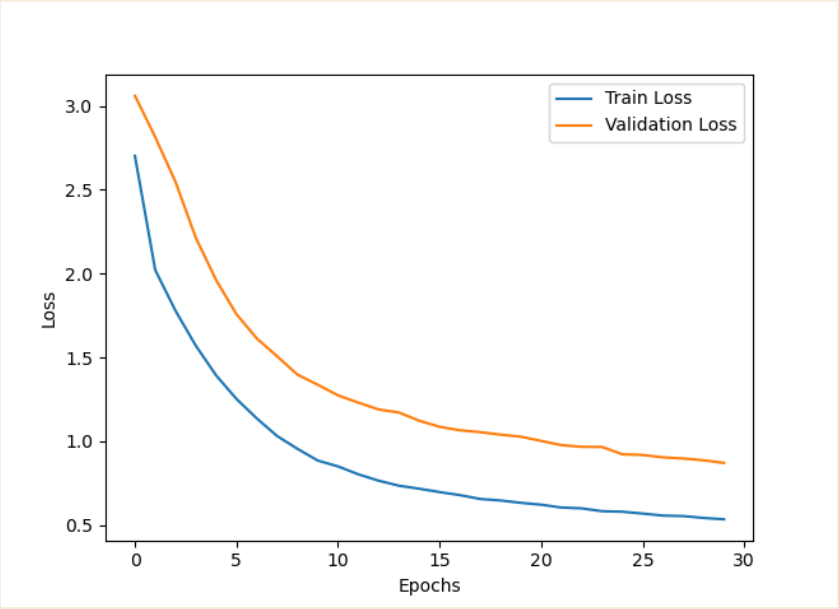
Structural Entropy on CNN



Structural Entropy on CNN

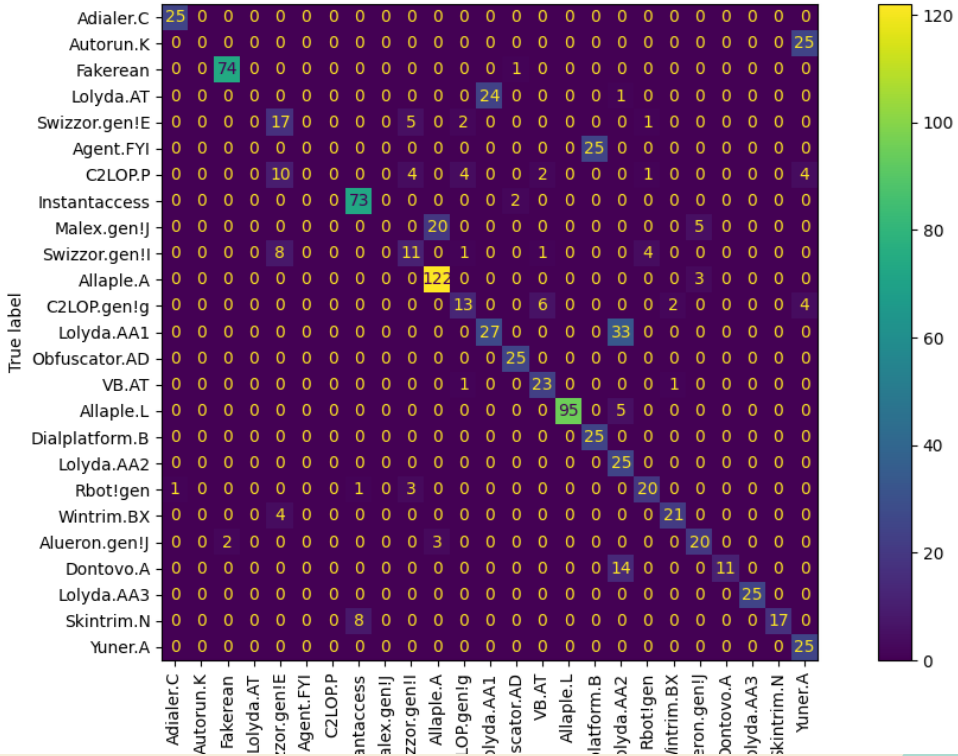


Accuracy



Loss

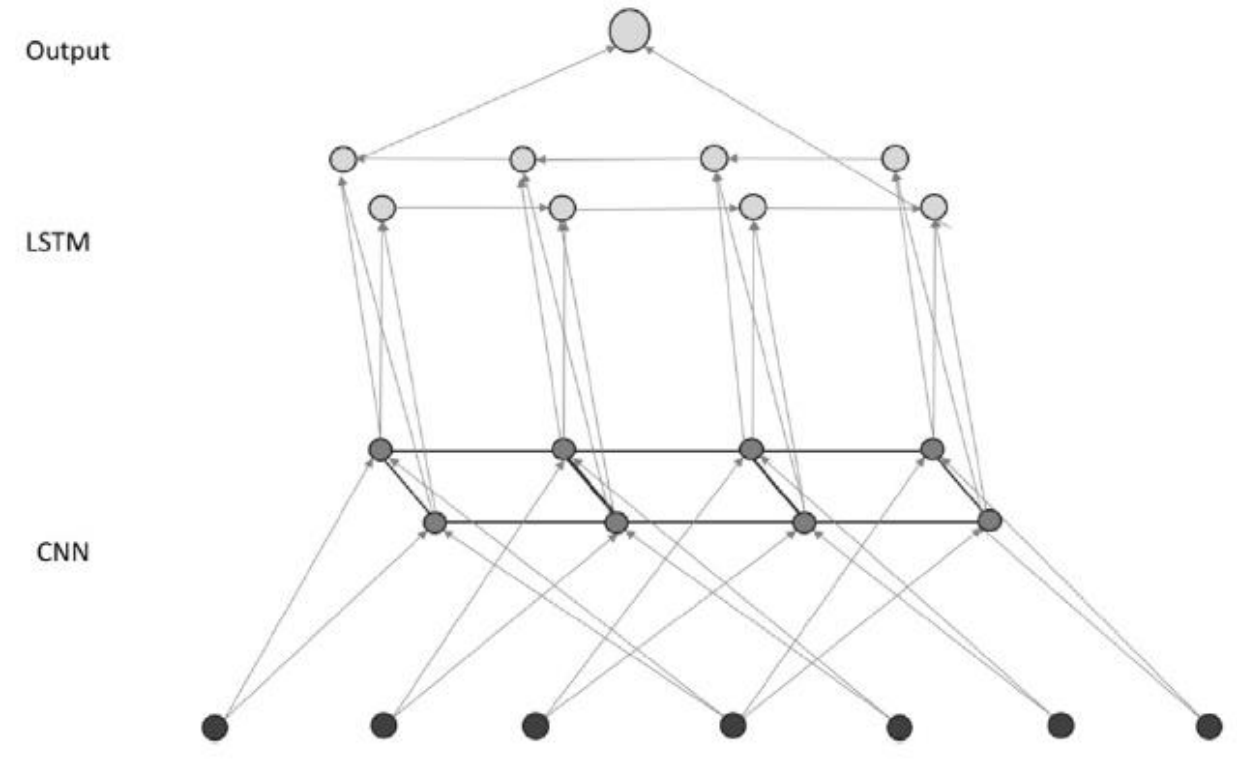
Confusion Matrix



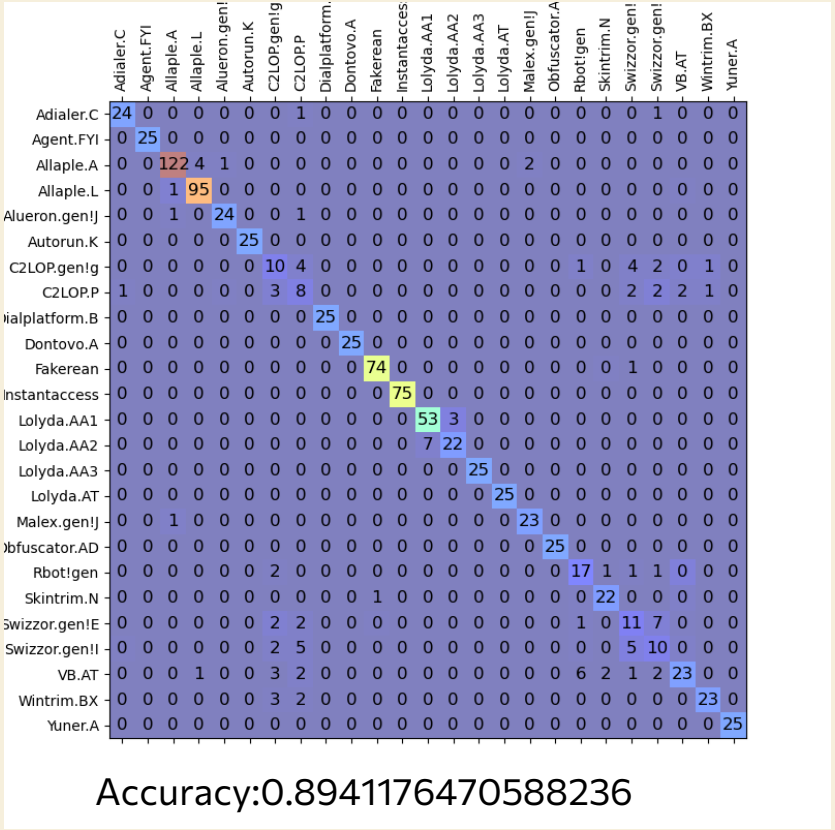
Deep learning at the shallow end: Malware classification for non-domain experts

		Accuracy (10-fold)	LogLoss	Macro F1 (10-fold)	Accuracy (5-fold)	F1 score (5-fold)				
24	**CNN BiLSTM - Reb Sampl**				98.20	96.05	Deep learning at the shallow end: Malware classification for non-domain experts		2018	LSTM

Deep learning at the shallow end: Malware classification for non-domain experts



Confusion Matrix



Accuracy:0.8941176470588236

結論

- Malware stored in image helps us analyzing malware
- Based on the result of classifying malware with dataset Malimg, first paper[1] performs the best, while second paper[2] performs the worst

[1]Gibert, D., Mateu, C., Planes, J., & Vicens, R. (2019). Using convolutional neural networks for classification of malware represented as images. Journal of Computer Virology and Hacking Techniques, 15(1), 15-28.
[2]Gibert, D., Mateu, C., Planes, J., & Vicens, R. (2018, April). Classification of malware by using structural entropy on convolutional neural networks. In Proceedings of the AAAI Conference on Artificial Intelligence (Vol. 32, No. 1).

參考資料

1. Malware Classification using Deep Learning - Tutorial | Towards Data Science
2. Kalash, M., Rochan, M., Mohammed, N., Bruce, N. D., Wang, Y., & Iqbal, F. (2018, February). Malware classification with deep convolutional neural networks. In 2018 9th IFIP international conference on new technologies, mobility and security (NTMS) (pp. 1-5). IEEE.
3. L. Nataraj, S. Karthikeyan, G. Jacob, and B. Manjunath, “Malware images: visualization and automatic classification,” in Proceedings of the 8th international symposium on visualization for cyber security. ACM, 2011, p. 4.
4. J. Drew, T. Moore, and M. Hahsler, “Polymorphic malware detection using sequence classification methods,” in Security and Privacy Workshops. IEEE, 2016, pp. 81–87.
5. J. Drew, M. Hahsler, and T. Moore, “Polymorphic malware detection using sequence classification methods and ensembles,” EURASIP Journal on Information Security, vol. 2017, no. 1, p. 2, 2017.
6. D. Gibert Llaurad´o, “Convolutional neural networks for malware classification,” Master’s thesis, Universitat Polit`ecnica de Catalunya, 2016.
7. M. Ahmadi, D. Ulyanov, S. Semenov, M. Trofimov, and G. Giacinto,“Novel feature extraction, selection and fusion for effective malwarefamily classification,” in Proceedings of the Sixth ACM Conference onData and Application Security and Privacy. ACM, 2016, pp. 183–194.
8. “Microsoft malware winners’ interview: 1st place, no to overfitting!”https://github.com/xiaozhouwang/kaggle Microsoft Malware/blob/master/Saynotooverfitting.pdf, 2017, accessed: 2017-04-22.
9. “Microsoft malware classification challenge (big 2015) first placeteam: Say no to overfitting,” http://blog.kaggle.com/2015/05/26/microsoft-malware-winners-interview-1st-place-no-to-overfitting/,2017, accessed: 2017-04-22.