Evaluating the Performance of ResNet Model Based on Image Recognition

Riaz Ullah Khan
School of Computer Science and Engineering
University of Electronic Science and Technology of China
+86-15520763595
rerukhan@gmail.com

Xiaosong Zhang
School of Computer Science and Engineering
University of Electronic Science and Technology of China
+86-18982067786
johnsonzxs@uestc.edu.cn

Rajesh Kumar
School of Computer Science and Engineering
University of Electronic Science and Technology of China
+86-15520777096
rajakumarlohano@gmail.com

Emelia Opoku Aboagye
School of Computer Science and Engineering
University of Electronic Science and Technology of China
+86-13258235906
eoaboagye@yahoo.co.uk

ABSTRACT

In this study, we have used two different Datasets to evaluate the performance of ResNet model. First dataset consists of images about healthcare data while second dataset consists of malware and benign _les. We performed experiments to predict cancer on the first dataset and detect malware on the second dataset. ResNet models i.e. Resnet18, ResNet50, ResNet101 and ResNet152 are investigated and tested which belong to Microsoft. The neural networks system has been turned out to be _t for approximating any ceaseless capacity, and all the more as of late profound neural systems (DNNs) have been observed to be viable in a few spaces, going from PC vision, speech recognition, to text processing. The purpose of this paper is to make recommendations prediction of the cancer disease adopting Neural networks and detecting the malware _les through the same ResNet model. We evaluated the performance of ResNet model on two different datasets.

CCS Concepts

• Theory of computation → Models of learning

Keywords

Malware Detection, ResNet, Deep Neural Network, Cancer Prediction, Image Recognition

1. INTRODUCTION

1.1 Background

Since the proposal of a fast learning algorithm for deep belief networks in 2006, the deep learning techniques have drawn a lot of research interests because of their inherent capability of overcoming the drawback of traditional algorithms dependent on hand-designed features. Deep learning approaches have additionally been observed to be reasonable for huge information investigation with effective applications to PC vision, design acknowledgment, speech recognition, pattern recognition and proposal frameworks [2]. Deep neural networks (DNNs) are techniques which hold the capability of learning from experience, it is powerful and enhances execution by adjusting to the changes in the environment, yet hard to train. The idea of Deep Learning taking is beginning from the examination on Artificial Neural Networks (ANNs) [4]. ANNs have become an active research area during the past few decades [8]. To construct a standard neural network (NN), it is essential to utilize neurons to produce real-valued activation and, by adjusting the weights, the NNs behave as expected. However, depending on the problems, the process of training an NN may take long causal chains of computations that increase its cost at the various stages. Back-propagation is a proficient inclination plunge calculation which has assumed a critical part in NNs since 1980 [6, 10]. It prepares the ANNs with an instructor based administered learning approach. Although the preparation accuracy is high, the execution of back-propagation when connected to the testing information won't not be satisfactory. As back-propagation relies upon neighborhood slant information with a self-assertive starting point, the computation oftentimes gets got in adjacent optima. Plus, if the traverse of the readiness data isn't adequately tremendous, NNs will face the issue of over-fitting. The essential advantages of DNNs are the probability of beneficial operation of a great deal of data and its ability to total up the outcome [3]. In this training calculation, the DNN, is utilized as a part of uses including grouping or function approximation, and it has been demonstrated that few classes of DNNs are all inclusive capacity approximations. Since the achievement in 2012 ImageNet rivalry [16] achieved by AlexNet. The primary section that utilized a Deep Neural Network (DNN) | a few different DNNs with expanding many-sided quality have been submitted to the test keeping in mind the end goal to accomplish better performance. In the ImageNet classification challenge, a definitive objective is to get the most astounding accuracy in a multi-class classification problem framework, paying little heed to the genuine derivation time [6]. We trust this has offered ascend to a few issues. This paper plans to think about best in class DNN architectures, in terms of computational requirements and accuracy and propose which one is ideal in terms of accuracy and running time for cancer prediction and Malware detection. This is the fact that, forward (MLP) selection techniques are believed to be better than in reverse techniques as far as computational productivity is concerned [13], [15]. However, we think

ICCAI 2018, March 12–14, 2018, Chengdu, China
© 2018 Association for Computing Machinery.
ACM ISBN 978-1-4503-6419-5/18/03$15.00
https://doi.org/10.1145/3194452.3194461

such techniques have a few noteworthy disservices, for example, being computationally excessively costly or occasionally incomprehensible, making it impossible to implement. We believe that, there is generally little work on utilizing DNNs for suggestion in the health sector and cyber security sector. We addressed the research problems by formalizing a neural systems approach for cancer collaborative filtering and malware detection.

1.2 Justification

System profundity is of urgent significance in neural network models, yet more profound systems are harder to prepare. The lingering learning structure facilitates the preparation of these systems, and empowers them to be generously deeper; leading to enhanced execution in both visual and non-visual undertakings. These remaining systems are significantly more profound than their \plain" partners, yet they require a comparative number of parameters (weights). The performance of ResNet model and its sub-models is assessed on different datasets to improve the results by adding number of parameters (Layers).

1.1.1. Cancer Prediction

Disease forecast is key as the survival of the patient relies upon opportune intercessions. This assumes, its forecast requires quick and strong models for such characteristic events is beneficial inquiring about. It is well taking note of that; ebb and ow inquire about is moving from framework investigation of little world systems to that of a huge number of hubs for expansive scale information preparing. Profound Multi-Layer Perceptron with improved advancement includes that is powerful and adaptable to upgrade such operations is basic.

1.1.2. Malware Detection

Malware is developing in the immense volume consistently, we utilized picture handling procedure so as to enhance exactness and execution. Picture handling procedure investigations malware parallels as dark scale pictures and opcode picture method. The past research Nataraj [7] proposed a gray-scale picture system to characterize malware utilizing picture preparing strategy. Some of develop image preparing methods are generally utilized for protest acknowledgment e.g. Taobao is well known shopping site in china which Discover's the item, utilizing image recognition method. This strategy performs high accuracy. In this study, we changed over parallel code to opcode pictures for perceiving malwares which save the similitude variation pictures. We thought about ResNet model to accomplish better execution as far as speed and accuracy.

1.3 Problem

With arrange profundity expanding, exactness and accuracy get soaked (which may be obvious) and after that debases quickly. Surprisingly, such debasement isn't caused by over-fitting, and adding more layers to an appropriately profound model prompts higher training losses.

2. DEEP NEURAL NETWORK PREDICTGION MODEL

2.1 Deep Neural Network for Cancer Prediction

We treat cancer prediction as an emergency issue and so formulate our problem with some initial considerations; fault tolerant contemplation for equipment, programming, and system security are basic territories in crisis circumstances as they altogether influence the effectiveness of the correspondence, and many key administration plans have been proposed to moderate the imperatives [11]. In case of cancer diagnosis, let be the probability of malignancy cells developing, at that point, the matrix would be influenced by $1-\varphi$, where φ is any random value within the prediction range. Let A be the damage matrix whose elements depict the level of damage to the cells caused by the disease and is defined as;

$$A = (1 - \varphi) \qquad (1)$$

The damage of disease cells will thus bring about the failure of the of the influenced cells and other life organs and matrix is defined with delineate the ag status of the cancer cells which are utilized as new created association matrix.

$$M_{i,j} = \begin{cases} 1, y_{i,j} \leq \alpha_L \\ 0, y_{i,j} \geq \alpha_H \\ \frac{\alpha_L}{\alpha_{i,j}}, \alpha_L < y_{i,j} < \alpha H \end{cases} \qquad (2)$$

Where αL represents the lower cancer impact and αH represents the higher cancer impact thresholds. To discover the network with the most extreme survival likelihood, another set of matrices is characterized after the damage. To enhance expectation rate after harm caused by the cancer cells, the expectation matrix is presented whose components demonstrate status of any expectation of survival. If J is the hope matrix, and is the risky matrix, then $J = G.,Er = (\mathrm{Ce} - \emptyset 2)J$, where matrix N and F as already defined above, is the total number of safe cells available for treatment and $\mathcal{P}hi2$ is the probability of additional error that miners may committed in the prediction task.

To allow a full neural treatment of synergistic filtering, we adopt a multi-layer [8] to draw the interaction between patient and image by $\mathcal{C}_p i$, where the yield of one layer fills in as the contribution of the following one. The base info layer comprises of two element vectors v_p^P and v_i^I that depict patient $\mathcal{P}$ and image i, individually. Over the information layer is the implanting layer; it is a completely associated layer that tasks the picture portrayal to a thick vector. The got tolerant picture installing can be viewed as the inert vector for patient (picture) with regards to dormant factor show. The patient inserting and picture implanting are then encouraged into a multi-layer neural design, which we term as tumor profound neural cooperative filtering layers, to delineate inert vectors to forecast scores. Each layer of the profound neural CF layers can be modified to find certain inert structures of interactions between user and item. The measurement of the last concealed layer Y (hidden layer) decides the model's capacity. The last output layer is the anticipated score $\overset{\wedge}{c_{pi}}$, and preparing is performed by limiting the point-wise misfortune among $\overset{\wedge}{c_{pi}}$ and its target value C_{pi}. We now figure the NCF's prescient model as;

$$\overset{\wedge}{c_{pi}} = f(A^T v_p^P, B^T v_i^I | A, B, \theta f) \qquad (3)$$

Where $A \epsilon R^{M \times K}$ and $B \epsilon R^{N \times K}$ meaning the inert factor lattice for patients and pictures, separately; and θf means that the model parameters of the association function f. Since the function f is defined as a multi-layer neural network, it can be defined as;

$$f A^T v_p^P, B^T v_i^I = \theta_{out}(\theta_y(...\theta_2(\theta_1(A^T v_p^P, B^T v_i^I))...)) \qquad (4)$$

Where θout and θy individually indicate the mapping capability for the yield layer and x th neural collaborative filtering (CF) layer, and there are Y neural CF layers altogether.

2.2 Deep Neural Network for Malware Detection

Malware classified in different families has multiple characteristics or features. Many authors used machine learning models such as Regression, K-nearest-neighbour, Random Forest etc. Main disadvantage of using machine learning is, features extraction is manual. Tong, Abadi and Krizhevsky [1], [5], [14] gave an overview of different machine learning techniques that were previously proposed for malware detection. Unlike Machine Learning, Deep learning skips the manual steps of extracting features. For instance, we can feed directly images and videos to the deep learning algorithm, which can predict the object. In this way deep learning model is more intelligent rather than machine learning model. We used convolutional neural networks because it is reliable, and it can be applied to the entire image at a time and then we can assume they are best to use for feature extraction. Recently Constitutional Neural Networks [9], [12] is the new approach to detect malware by using image based similarity technique. Its automated image comparison helps analysts to visually identify common code portions or specific instruction blocks within a sample. In this work we used three different datasets and compared the accuracy. Secondly, we used different techniques to prepare datasets for training and testing purposes. We trained and tested the CNN model for better understanding of the malware behaviour. Overall, we show that our proposed approach constitutes a valuable asset in the fight against malware. Figure 1 gives a brief overview to the different stages i.e. from training to malware detection.

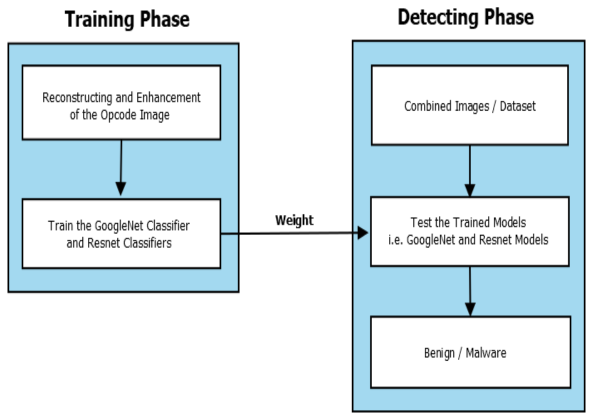
Training Phase
Detecting Phase
Reconstructing and Enhancement of the Opcode Image
Train the GoogleNet Classifier and Resnet Classifiers
Weight
Combined Images / Dataset
Test the Trained Models i.e. GoogleNet and Resnet Models
Benign / Malware

Figure 1. Architecture of proposed Method for Malware Detection.

In this design we divided model in two phases i) Training phase and ii) Detection phase. For the training and the detection of malware we used CNN model, as shown in Figure 1. We prepare the dataset using different techniques shown in data preparation section. The output of the data preparation section is \image files". Images have binary labels i.e. either benign or malware. we used supervised learning model in which the features are extracted automatically. The detection phase is shown in Figure 1. The same exe file convert in image and trained classifier detect the malicious code.

3. COLLECTION OF DATASET CANCER DATASET

We collected two datasets from different sources one from Chengdu Sichuan Cancer Hospital, other from UESTC hospital. We have collected 2000 patient's data that includes many samples which is shown in Figure 2. This dataset comprises breast cancer, Chest cancer and other types of cancers. We split dataset into two parts one is testing and other for training. We split dataset 20% for validation and testing and 80% for training.

3.1 Malware and Benign Dataset

We have collected two datasets from different sources. One of them is malicious dataset from Microsoft Malware Classification Challenge. We also have collected 3000 benign files from different sources. Figure 3 clearly show the images of malware and benign i.e. left image is malware and right image is benign image. Both datasets are discussed briefly in the following discussions.

1. Microsoft Malware Classification Challenge Dataset: The Microsoft dataset contains 9 classes for training and testing purposes. Microsoft provided 500GB of data which includes 21741 malware samples. 10868 of samples are used for training, and the remaining samples are used for testing.
2. Benign files: We collected 3000 benign _les from different sources.

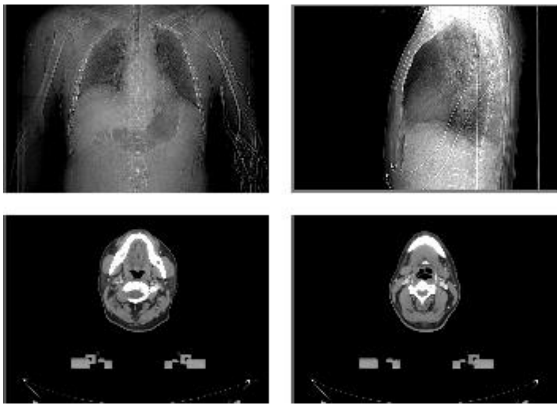

Figure 2. X-Ray Images of Patients.

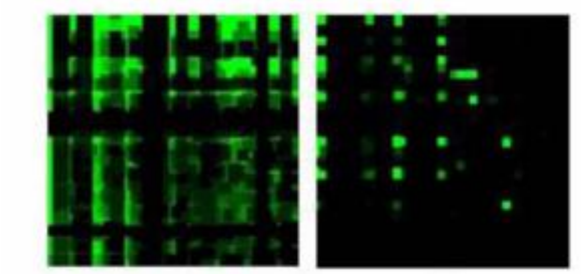

Figure 3. Malware (Left) and Benign (Right) Images.

3.2 Environment Setup

Ubunto OS with 8 GB RAM is used to perform tests. We used Python programming language to perform the experiments. Python packages and libraries such as Tensor Flow, Docker Server, Anaconda are used which helped to analyse the test results of ResNet Model. Four ResNet models were evaluated on datasets and the results are further discussed in Section 4. Microsoft Excel 2016 is used to draw statistical charts.

4. EXPERIMENTS AND RESULTS

We run our experiments on natural reliable real data sets from Chengdu Sichuan Cancer Hospital, from UESTC hospital and Microsoft Malware Classification Challenge. The images contained the chest and other parts of patients diagnosed with cancer for a period of 10 years and Malware samples. We adopted the Deep Neural network model i.e. ResNet model. It was observed that, ResNet model has tremendous performance on cancer dataset as compare to malware dataset. We are tempted to believe that, if the data sets were larger than we have experimented, ResNet152 would have performed better. However, ResNet (18, 50 and 101) really performed better in terms of prediction accuracy on cancer data which is observed in Table 1 and Figure 4. It however, performed poorly in terms of running time on malware dataset which is observed in Table 4 and Figure 5. Be that as it may, when just a restricted measure of preparing information is accessible, all the more capable models are required to accomplish an improved learning capacity. It is along these lines of incredible essentially to think about how to plan deep models to gain from less preparing information, particularly for discourse and visual acknowledgment frameworks. This was apparent in our explored different avenues regarding ResNet Uses of optimization algorithms to adjust the network parameters: The technique to modify the parameters in machine learning calculations is a rising theme in software engineering. In DNNs, an extensive number of parameters should be balanced. Additionally, with an expanding number of shrouded hubs, the calculation is more probable get caught in the nearby ideal. Enhancement procedures, for example, the PSO, are hence required to maintain a strategic distance from this issue. The pro- posed preparing calculation ought to have the capacity to extricate the highlights naturally and diminish the loss of data to moderate both the scourge of dimensional and the local optimum.

Table 1. Comparison Results of different ResNet Models on Cancer Dataset

Models	Training Accuracy	Testing Accuracy	Prediction Time
ResNet18	0.9719	0.84	1131 s
ResNet50	0.9811	0.98	1396 s
ResNet101	0.982	0.98	1844 s
ResNet152	0.9876	0.98	2131 s

Table 2. Comparison Results of different ResNet Models on Malware Dataset

Models	Training Accuracy	Testing Accuracy	Prediction Time
ResNet18	0.83	0.87	2701 s
ResNet50	0.8662	0.8095	5580 s
ResNet101	0.8594	0.7884	6112 s
ResNet152	0.8798	0.8836	9248 s

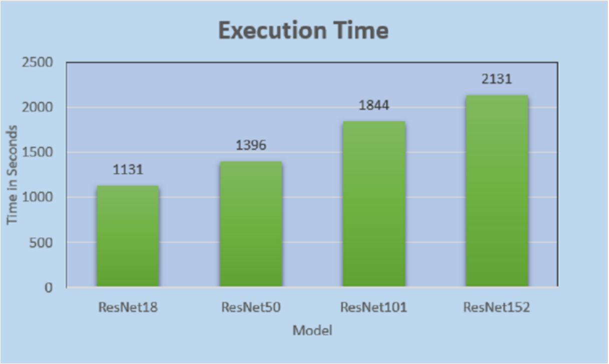

Figure 4. Prediction time of ResNet Models on Cancer Dataset (Time in Seconds).

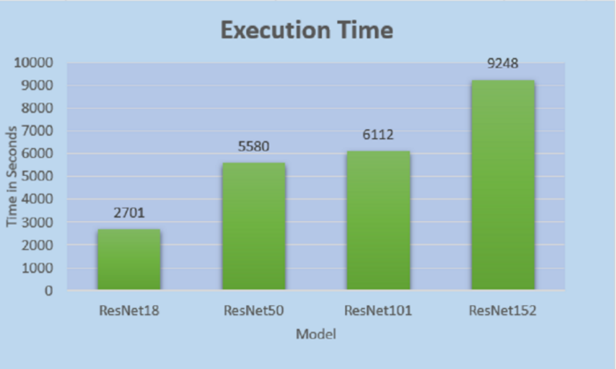

Figure 5. Prediction time of ResNet Models on Malware Dataset (Time in Seconds).

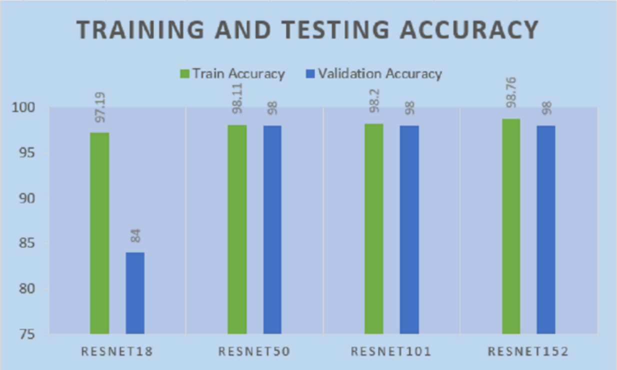

Figure 6. Comparison of the Training and Testing accuracy of ResNet models on Cancer Dataset.

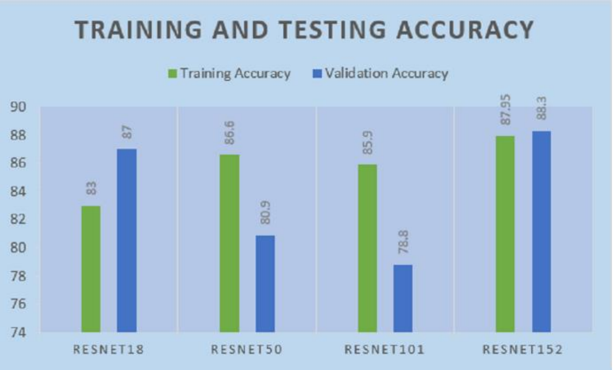

Figure 7. Comparison of the Training and Testing accuracy of ResNet models on Malware Dataset.

5. CONCLUSION

With the advancement of enormous information examination, deep learning has been utilized for situations where huge measures of unsupervised information are included. As a proficient apparatus for huge information investigation, the deep learning procedure has made extraordinary progress with tremendous measures of unlabelled preparing information. We therefore conclude our study by proposing ResNet for image classification and prediction tasks and deduce that, ResNet is a good recommendation predictor for the survival-ability of cancer patients. The lower the Loss, the better a model. The loss is calculated on training and validation and its interpretation is how well the model is doing for these two sets. Loss is not in percentage as opposed to accuracy and it is a summation of the errors made for each example in training or validation sets. In terms of model training accuracy 152layer ResNet model achieved top most accuracy.

6. REFERENCES

[1] Abadi, M., Barham, P., Chen, J., Chen, Z., Davis, A., Dean, J., Devin, M., Ghemawat, S., Irving, G., Isard, M., Kudlur, M., Levenberg, J., Monga, R., Moore, S., Murray, D. G., Steiner, B., Tucker, P., Vasudevan, V., Warden, P., Wicke, M., Yu, Y., Zheng, X., and Brain, G. 2016. TensorFlow: A System for Large-Scale Machine Learning. *12th USENIX Symposium on Operating Systems Design and Implementation* (2016).

[2] Gong, Y., Leung, K. H. T., Toshev, A. T., Ioffe, S., and Jia, Y. 2017. Ranking approach to train deep neural nets for multilabel image annotation, *Google Patent*s.

[3] He, K., Zhang, X., Ren, S., and Sun, J. 2015. Delving deep into rectifiers: Surpassing human-level performance on ImageNet classification. *In Proceedings of the IEEE international conference on computer vision*, pp. 1026-1034.

[4] He, X., Liao, L., Zhang, H., Nie, L., Hu, X., and Chua, T.-S. 2017. Neural Collaborative Filtering. *In Proceedings of the 26th International Conference on World Wide Web - WWW '17 (2017)*, pp. 173-182.

[5] Krizhevsky, A., Sutskever, I., and Hinton, G. E. 2012. ImageNet Classification with Deep Convolutional Neural Networks. *In Proceedings of the Neural Information Processing Systems*, pp 1097 – 1105

[6] Liu, W., Wang, Z., Liu, X., Zeng, N., Liu, Y., and Alsaadi, F. E. 2017. A survey of deep neural network architectures and their applications. *Neurocomputing*. Vol. 234, pp 11-26.

[7] Nataraj, L., Yegneswaran, V., Porras, P., and Zhang, J. 2011. A Comparative Assessment of Malware Classification Using Binary Texture Analysis and Dynamic Analysis. *Proceedings of the 4th ACM Workshop on Security and Artificial Intelligence*, pp 21-30.

[8] Parkhi, O. M., Vedaldi, A., Zisserman, A. 2015. Deep Face Recognition. *In BMVC*, vol. 1, p. 6.

[9] Paulin, M., Douze, M., Harchaoui, Z., Mairal, J., Perronin, F., and Schmid, C. 2015. Local convolutional features with unsupervised training for image retrieval. *In Proceedings of the IEEE International Conference on Computer Vision*, pp. 91-99.

[10] Rajkomar, A., Lingam, S., Taylor, A. G., Blum, M., and Mongan, J. 2017. High-throughput classification of radiographs using deep convolutional neural networks. *Journal of digital imaging*, Vol. 30(1), pp 95-101.

[11] Ramachandra, R., McGrew, S. Y., Baxter, J. C., Howard, J. R., and Elmslie, K. S. 2013. NaV 1.8 channels are expressed in large, as well as small, diameter sensory afferent neurons. *Channels (Austin, Tex.)* Vol. 7 (1), pp 34-47.

[12] Simonyan, K., and Zisserman, A. 2015. Very deep convolutional networks for large-scale image recognition. *arXiv preprint arXiv:1409.1556*.

[13] Szegedy, C., Ioffe, S., Vanhoucke, V., and Alemi, A. A. 2017. Inception-v4, Inception-ResNet and the Impact of Residual Connections on Learning. *In AAAI (2017)*, pp. 4278-4284.

[14] Tong, F., and Yan, Z. 2017. A hybrid approach of mobile malware detection in Android. *Journal of Parallel and Distributed Computing*. Vol 103, pp 22 – 31

[15] Vervliet, N., Debals, O., Sorber, L., and De Lathauwer, L. 2014. Breaking the curse of dimensionality using decompositions of incomplete tensors: Tensor-based scientific computing in big data analysis. *IEEE Signal Processing Magazine* Vol. 31(5), pp 71-79.

[16] Wu, S., Zhong, S., and Liu, Y. 2017. Deep residual learning for image steganalysis. *Multimedia Tools and Applications*.