ABSTRAK

Kebocoran data akibat *malware* menjadi salah satu kejahatan siber yang paling banyak dilaporkan pada tahun 2023, dengan *malware* berperan sebagai perangkat lunak yang dapat merusak sistem komputer. *Malware* mudah diluncurkan karena dapat dibuat dari varian yang sudah ada, menyebabkan kerugian besar di berbagai bidang. Maka dari itu, perlu dilakukan upaya untuk meminimalisasi kerugian yang ditimbulkan oleh *malware*, salah satunya adalah pengklasifikasian *malware*. Pengklasifikasian *malware*, termasuk metode berbasis citra seperti *binary visualization*, dinilai lebih efisien dibanding teknik analisis statis dan dinamis karena tidak memerlukan *reverse engineering*. Teknik berbasis citra ini memanfaatkan kesamaan citra *malware* dalam *family* yang sama untuk diklasifikasikan oleh model *machine learning*, seperti CNN. Namun, CNN dapat menghadapi masalah *vanishing gradient* pada model dengan layer yang dalam, yang dapat diatasi oleh arsitektur ResNet dengan *skip connection*, sehingga memungkinkan penggunaan hingga ratusan layer tanpa mengurangi akurasi.

Pada penelitian ini dilakukan pengklasifikasian citra *malware* pada *dataset* MaleVis menggunakan model arsitektur *transfer learning* ResNet50 dan model yang telah dilakukan pembaruan, yaitu ResNet-RS50 untuk mengetahui perbandingan performa di antara keduanya. Terdapat 26 total kelas pada *dataset* yang terdiri dari 25 kelas merupakan citra dari *malware family* yang telah dikenali dan 1 kelas merupakan citra dari *file* bukan *malware*. *Dataset* mengandung data sejumlah 14226 data yang terdiri dari 9100 data *training* dan 5126 data *testing*. Model diuji menggunakan metode Hold-Out, maka dari itu data *training* dibagi kembali menjadi data *training* dan data *validation* dengan rasio 7:3. Untuk perbandingan performa, kedua model diberikan *hyperparameter* yang sama, yaitu kombinasi dari *epoch* sejumlah 25 dan 50 dan *batch size* senilai 32 dan 64 sehingga menghasilkan 8 kombinasi pengujian.

Dari 8 kombinasi pengujian yang ada, diketahui bahwa model ResNet-RS50 dengan *epoch* sejumlah 25 dan *batch size* senilai 64 memiliki performa terbaik dengan akurasi 86,95%, presisi 90,75%, *recall* 93,98%, f-1 *score* 90,38%, dan durasi pelatihan selama 3,56 jam. Hasil dari performa 8 kombinasi pengujian kemudian disajikan dalam bentuk grafik sehingga diketahui bahwa kedua model tidak memiliki perbedaan performa yang signifikan, namun model ResNet-RS50 sedikit lebih unggul jika dilatih menggunakan *epoch* sejumlah 25 dan model ResNet50 sedikit lebih unggul jika dilatih menggunakan *epoch* sejumlah 50. Keunggulan tersebut ditandai dengan akurasi yang lebih tinggi dengan durasi pelatihan yang kurang lebih sama.

Kata kunci: *Malware, binary visualization, CNN, ResNet, MaleVis, transfer learning, ImageNet, epoch, batch size*

ABSTRACT

Data breaches caused by malware became one of the most reported cybercrimes in 2023, with malware acting as software capable of damaging computer systems. Malware is easily launched because it can be created from existing variants, causing significant losses across various sectors. Therefore, it is necessary to make efforts to minimize the damage caused by malware, one of which is through malware classification. Malware classification, including image-based methods like binary visualization, is considered more efficient than static and dynamic analysis techniques because it does not require reverse engineering. This image-based technique leverages the visual similarity of malware within the same family for classification by machine learning models such as CNN. However, CNN may face vanishing gradient issues in deep-layered models, which can be addressed by ResNet architecture using skip connections, allowing the use of hundreds of layers without reducing accuracy.

This research performs malware image classification on the MaleVis dataset using the ResNet50 transfer learning architecture and its updated model, ResNet-RS50, to compare their performance. The dataset contains 26 total classes, 25 of which are images of known malware families and 1 class representing non-malware files. The dataset comprises 14,226 images, with 9,100 for training and 5,126 for testing. The Hold-Out method is used to split the training data into training and validation sets with a 7:3 ratio. For performance comparison, both models are tested using the same hyperparameters, consisting of combinations of 25 and 50 epochs and batch sizes of 32 and 64, resulting in 8 test combinations.

Out of the 8 test combinations, the ResNet-RS50 model with 25 epochs and a batch size of 64 achieved the best performance, with an accuracy of 86.95%, precision of 90.75%, recall of 93.98%, F1 score of 90.38%, and a training duration of 3.56 hours. The results of the 8 tests are presented in graphical form, showing no significant performance difference between the two models. However, ResNet-RS50 performed slightly better when trained with 25 epochs, while ResNet50 performed slightly better when trained with 50 epochs. This advantage is marked by higher accuracy with approximately the same training duration.

Keywords: *Malware, binary visualization, CNN, ResNet, MaleVis, transfer learning, ImageNet, epoch, batch size*