BAB V
PENUTUP

5.1 Kesimpulan

Dalam penelitian ini pendekatan baru diterapkan dengan teknik *image processing* dengan algoritma *Convolutional Neural Network* dalam melakukan klasifikasi dari *malicious software*. Dari rangakaian tahapan penelitian dan analisis hasil pengujian yang telah dibahas maka dapat ditarik sebuah kesimpulan sebagai berikut :

1. Metode *Convolutional Neural Network* yang merupakan metode *deep learning* yang digunakan dalam bidang *image proocessing* mampu mengklasifikasikan *malicious software* yang telah dikonversi dalam bentuk citra.
2. Metode *Convolutional Neural Network* dengan penerapan *zero padding* secara efisien mengklasifikasikan *malware* dengan jenis varian kelas baru seperti *Trojan, Backdoor / Rootkit*, dan *Worm* yang menjadi masalah pada penelitian sebelumnya.
3. Implementasi *zero padding* pada model CNN terbukti menaikkan akurasi uji dan memperbaiki hasil uji penelitian sebelumnya dengan akurasi uji yang dihasilkan mencapai 99,04%.

5.2 Saran

Adapun saran yang diberikan pada penelitian ini sebagai berikut :

1. Menambahkan data citra pada *dataset* dengan kelas yang memiliki data yang relatif sedikit untuk melatih model CNN secara lebih dalam terhadap data *malware*.

2. Pengembangan dari model CNN pada penelitian ini dapat dilakukan dengan implementasi sistem yang bertujuan menanggulangi ancaman dari *malicious software*.
3. Penerapan variasi lain pada model CNN yang dibangun seperti menerapkan *Transfer Learning* dan penerapan *Cross Validation* pada evaluasi & validasi model.
4. Pengembangan model dengan menambahkan beberapa parameter sebagai pembanding guna untuk mendapatkan arsitektur yang lebih baik lagi.