

**Implementasi Model Deep Learning InceptionResNet-V2 Untuk Image
Classification Pada Malware**

Laporan Tugas Akhir

Diajukan Untuk Memenuhi
Persyaratan Guna Meraih Gelar Sarjana
Informatika Universitas Muhammadiyah Malang



Jafar Shodiq Djawas
201810370311068

Bidang Minat

Data Science

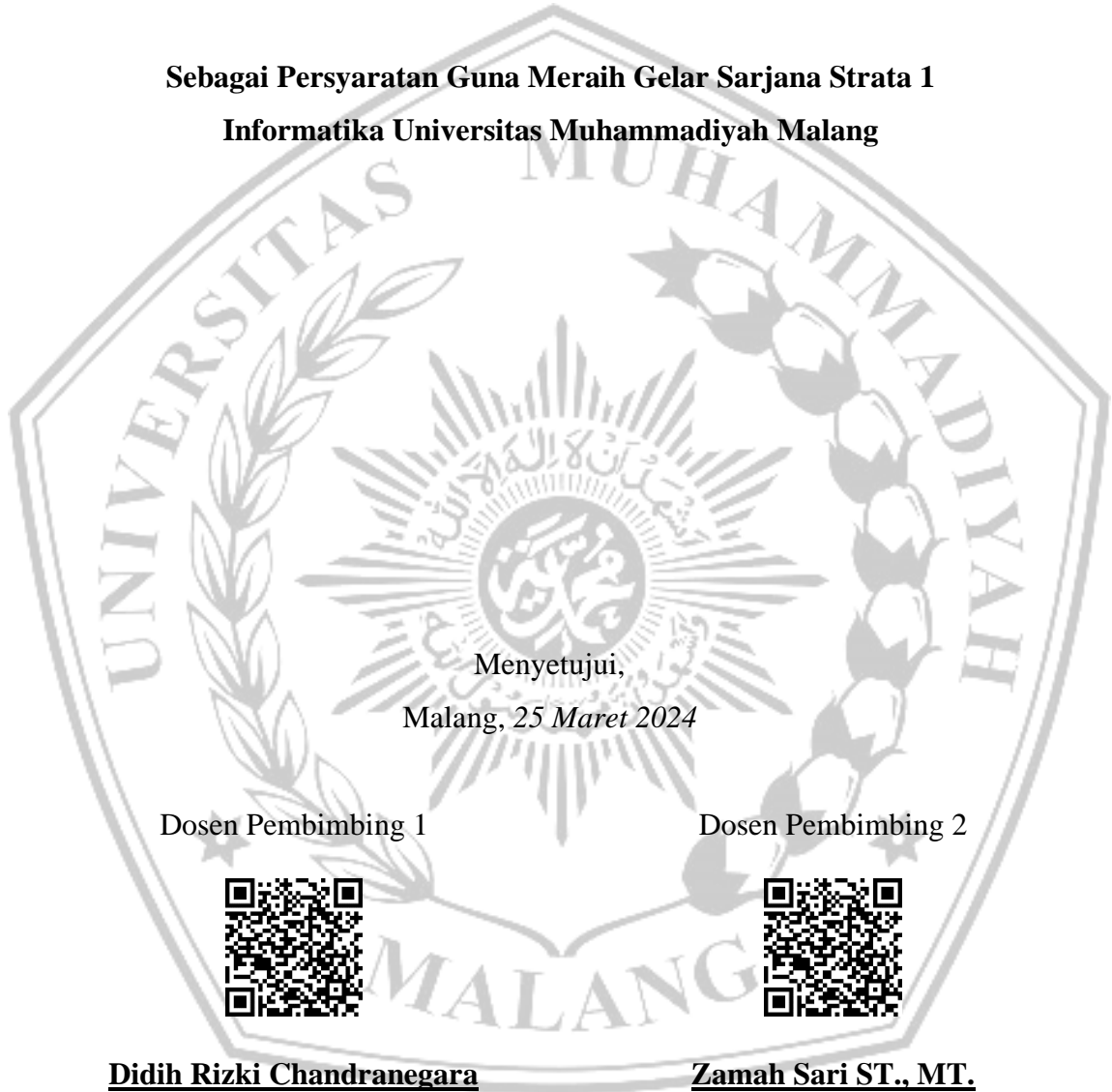
**PROGRAM STUDI INFORMATIKA
FAKULTAS TEKNIK
UNIVERSITAS MUHAMMADIYAH MALANG
2024**

LEMBAR PERSETUJUAN

**Implementasi Model Deep Learning InceptionResNet-V2 Untuk
Image Classification Pada Malware**

TUGAS AKHIR

**Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata 1
Informatika Universitas Muhammadiyah Malang**



Menyetujui,
Malang, 25 Maret 2024

Dosen Pembimbing 1



Didih Rizki Chandranegara

S.kom., M.Kom

NIP. 180302101992PNS.

Dosen Pembimbing 2



Zamah Sari ST., MT.

NIP. 10814100555PNS.

LEMBAR PENGESAHAN

Implementasi Model Deep Learning InceptionResNet-V2 Untuk Image Classification Pada Malware

TUGAS AKHIR

Sebagai Persyaratan Guna Meraih Gelar Sarjana Strata I
Informatika Universitas Muhammadiyah Malang

Disusun Oleh :

Jafar Shodiq Djawas

201810370311068

Tugas Akhir ini telah diuji dan dinyatakan lulus melalui sidang majelis penguji
pada tanggal 25 Maret 2024

Menyetujui,

Dosen Penguji 1



Ir. Denar Regata Akbi S.Kom., M.Kom.

NIP. 10816120591PNS.

Dosen Penguji 2



Hardianto Wibowo S.Kom., MT.

NIP. 10816120592PNS.

Mengetahui,

Ketua Jurusan Informatika



Ir. Galih Wasis Wicaksono S.kom. M.Cs.

NIP. 10814100541PNS.

LEMBAR PERNYATAAN

Yang bertanda tangan dibawah ini :

NAMA : Jafar Shodiq Djawas

NIM : 201810370311068

FAK./JUR. : Informatika

Dengan ini saya menyatakan bahwa Tugas Akhir dengan judul **“Implementasi Model Deep Learning InceptionResNet-V2 Untuk Image Classification Pada Malware”** beserta seluruh isinya adalah karya saya sendiri dan bukan merupakan karya tulis orang lain, baik sebagian maupun seluruhnya, kecuali dalam bentuk kutipan yang telah disebutkan sumbernya.

Demikian surat pernyataan ini saya buat dengan sebenar-benarnya. Apabila kemudian ditemukan adanya pelanggaran terhadap etika keilmuan dalam karya saya ini, atau ada klaim dari pihak lain terhadap keaslian karya saya ini maka saya siap menanggung segala bentuk resiko/sanksi yang berlaku.

Mengetahui,
Dosen Pembimbing

Malang, 25 Maret 2024
Yang Membuat Pernyataan



Didih Rizki Chandranegara S.kom.,
M.Kom

Jafar Shodiq Djawas

ABSTRAK

Klasifikasi malware citra adalah teknik yang digunakan untuk mengidentifikasi dan mengklasifikasikan jenis malware menggunakan citra yang dihasilkan oleh analisis dinamis dan statis. Metode klasifikasi malware citra yang paling umum digunakan adalah Convolutional Neural Network (CNN) yang dilatih menggunakan dataset malware citra. Penelitian ini bertujuan untuk mengembangkan model klasifikasi malware citra berbasis CNN dengan menggunakan metode InceptionResNet-V2. Dataset yang digunakan dalam penelitian ini terdiri dari total 9.029 sampel citra malware dari 25 kelas yang berbeda dari dataset Maling. Proses pengujian dilakukan dengan membagi dataset menjadi dua bagian: data test dan data train. Kami menggunakan dataset yang terdiri dari berbagai jenis malware untuk melatih dan menguji model kami. Kami juga melakukan beberapa teknik augmentasi citra seperti flipping dan cropping pada gambar untuk meningkatkan performa model kami. Penelitian ini menjalankan 2 skenario yang berbeda, skenario 1 menggunakan dataset asli dan skenario lainnya menggunakan dataset yang diambil sampelnya secara acak. Dalam penelitian ini, model yang dihasilkan dari skenario 1 mencapai akurasi sebesar 87.5% dan pada skenario 2 mencapai akurasi sebesar 85.1% dalam mengklasifikasikan citra malware. Penelitian ini diharapkan dapat memberikan kontribusi pada pengembangan teknik klasifikasi malware citra yang lebih akurat dan efektif dalam mendeteksi ancaman malware pada sistem komputer.

Kata Kunci: *Klasifikasi Citra, Malware, Deep Learning, CNN, Siber*

ABSTRACT

Image malware classification is a technique used to identify and classify types of malware using images generated by dynamic and static analysis. The most commonly used method for image malware classification is Convolutional Neural Network (CNN) trained using a dataset of malware images. This research aims to develop a CNN-based image malware classification model using the InceptionResNet-V2 method. The dataset used in this research consists of a total of 9,029 malware image samples from 25 different classes from the Maling dataset. The testing process is carried out by dividing the dataset into two parts: test data and train data. We use a dataset consisting of various types of malware to train and test our model. We also perform several image augmentation techniques such as flipping and cropping to improve our model's performance. This research runs two different scenarios, scenario 1 uses the original dataset and the other scenario uses a randomly sampled dataset. In this research, the model generated from scenario 1 achieved an accuracy of 87.5% and scenario 2 achieved an accuracy of 85.1% in classifying malware images. This research is expected to contribute to the development of more accurate and effective image malware classification techniques in detecting malware threats on computer systems.

Keywords: *Image Classification, Malware, Deep Learning, CNN, Cyber*

LEMBAR PERSEMBAHAN

Assalamualaikum Wr. Wb. Puji syukur penulis panjatkan kehadirat Allah SWT atas segala rahmat, karunia, dan bimbingan-Nya yang telah diberikan selama penulisan skripsi ini. Penulis juga mengucapkan terima kasih kepada beberapa pihak yang telah memberikan dukungan dan bantuan selama proses penulisan skripsi ini, antara lain:

1. Keluarga tercinta Ayah, Mama, Annisa yang selalu memberikan doa, dukungan, dan semangat kepada penulis selama proses penulisan skripsi.
2. Bapak / Ibu Dosen Jurusan Informatika Universitas Muhammadiyah Malang.
3. Dosen pembimbing, Bapak Didih Rizki Chandranegara, S.Kom., M.Kom. dan Bapak Zamah Sari, ST., MT yang telah memberikan bimbingan, arahan, dan masukan yang sangat berharga dalam penulisan skripsi ini.
4. Teman-teman seperjuangan di kampus yang selalu memberikan semangat, dukungan, dan motivasi kepada penulis dalam menyelesaikan skripsi ini.

Akhir kata, terima kasih banyak. Wassalamualaikum Wr. Wb.

Malang, 22 Februari 2024



Jafar Shodiq Djawas

KATA PENGANTAR

Dengan memanjatkan puji syukur kehadiran Allah SWT. Atas limpahan rahmat dan hidayah-NYA sehingga peneliti dapat menyelesaikan tugas akhir yang berjudul :

“ IMPLEMENTASI MODEL DEEP LEARNING INCEPTIONRESNET-V2 UNTUK IMAGE CLASSIFICATION PADA MALWARE ”

Di dalam tulisan ini disajikan pokok-pokok bahasan yang meliputi dataset image malware, preprocessing menggunakan data augmentation, Image Segmentation menggunakan teknik balancing dataset dan imbalancing dataset, CNN dengan model pretrained InceptionResnet-V2, Evaluasi model dan perbandingan hasil dari skenario yang diujikan antara dataset balance dan imbalance.

Penulis menyadari bahwa masih banyak kekurangan dalam penulisan skripsi ini, baik dari segi isi maupun penulisan. Oleh karena itu, penulis sangat mengharapkan saran, kritik, dan masukan yang membangun dari semua pihak demi perbaikan dan pengembangan penulisan selanjutnya.

Malang, 22 Februari 2024



Jafar Shodiq Djawas

DAFTAR ISI

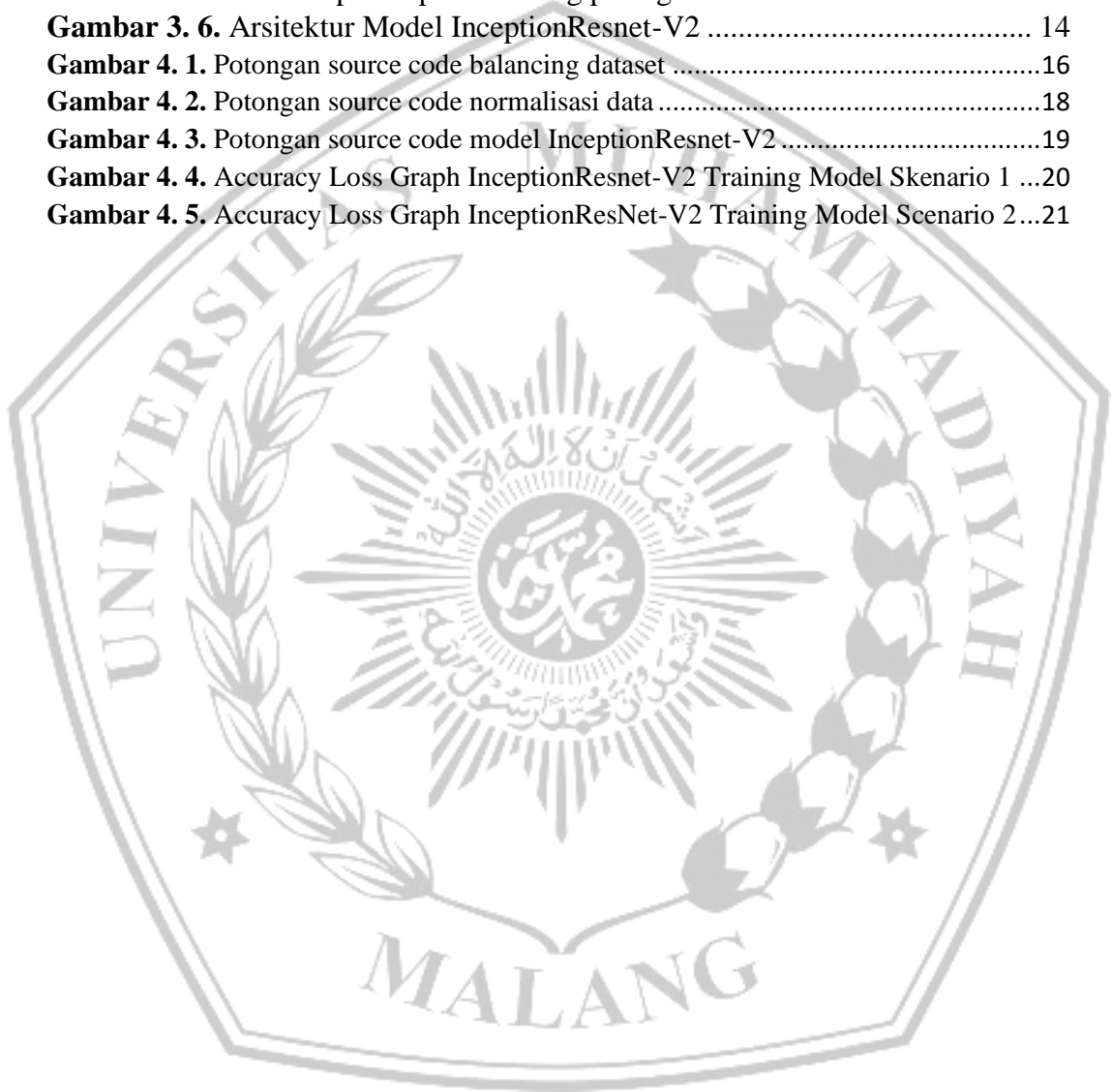
LEMBAR PERSETUJUAN	1
LEMBAR PENGESAHAN	2
LEMBAR PERNYATAAN	3
ABSTRAK	4
ABSTRACT	5
LEMBAR PERSEMBAHAN	6
KATA PENGANTAR	7
DAFTAR ISI	8
DAFTAR GAMBAR	10
DAFTAR TABEL	11
BAB I PENDAHULUAN	1
1.1. Latar Belakang	1
1.2. Rumusan Masalah	3
1.3. Tujuan Penelitian	3
1.4. Batasan Masalah	4
BAB II KAJIAN PUSTAKA	5
2.1. Studi Literatur	5
2.2. Convolutional Neural Network	6
2.3. InceptionResnet-V2	7
BAB III METODOLOGI PENELITIAN	8
3.1. Tahapan Penelitian	8
3.2. Dataset	9
3.3. Pre-processing Dataset	10
3.3.1. Balancing Dataset	10
3.3.2. Grayscale Dataset	10
3.3.3. Resizing Dataset	11
3.3.4. Rescaling Dataset	12
3.4. Pembuatan Model	13
3.4.1. InceptionResnet-V2	13
BAB IV HASIL DAN PEMBAHASAN	16
4.1. Persiapan dan Pengolahan Dataset	16
4.2. Model CNN InceptionResnet-V2	17
4.3. Pengujian	18

4.3.1 Skenario 1.....	19
4.3.2 Skenario 2.....	20
4.4 Rangkuman Hasil Pengujian.....	22
BAB V KESIMPULAN.....	24
5.1 Kesimpulan	24
5.2 Saran.....	24
DAFTAR PUSTAKA.....	25



DAFTAR GAMBAR

Gambar 2. 1. Arsitektur CNN.....	6
Gambar 2. 2. Arsitektur Model InceptionResnet-V2	7
Gambar 3. 1 Alur Tahapan Penelitian	8
Gambar 3. 2. Contoh Gambar Dataset Malware	10
Gambar 3. 3. Contoh hasil proses grayscale pada dataset.....	11
Gambar 3. 4. Ilustrasi penerapan resizing pada gambar.....	12
Gambar 3. 5. Ilustrasi penerapan rescaling pada gambar	13
Gambar 3. 6. Arsitektur Model InceptionResnet-V2	14
Gambar 4. 1. Potongan source code balancing dataset	16
Gambar 4. 2. Potongan source code normalisasi data	18
Gambar 4. 3. Potongan source code model InceptionResnet-V2	19
Gambar 4. 4. Accuracy Loss Graph InceptionResnet-V2 Training Model Skenario 1 ...	20
Gambar 4. 5. Accuracy Loss Graph InceptionResNet-V2 Training Model Scenario 2...21	



DAFTAR TABEL

Tabel 2. 1. Studi Terdahulu	5
Tabel 4. 1. Perbandingan hasil dataset.....	17
Tabel 4. 2. Hasil Akurasi Skenario 1	19
Tabel 4. 3. Hasil Model Evaluation pada Skenario 1	20
Tabel 4. 4. Hasil Akurasi Skenario 2.....	21
Tabel 4. 5. Hasil Model Evaluation pada Skenario 2.....	21
Tabel 4. 6. Hasil Akurasi Pada Setiap Skenario	22
Tabel 4. 7. Hasil Akurasi Dengan Penelitian Sebelumnya.....	22



DAFTAR PUSTAKA

- [1] Choi, S., Bae, J., Lee, C., Kim, Y., & Kim, J. (2020). Attention-based automated feature extraction for malware analysis. *Sensors (Switzerland)*, 20 (10). <https://doi.org/10.3390/s20102893>
- [2] Purnamawati, A., Nugroho, W., Putri, D., & Hidayat, W. F. (2020). *InfoTekJar : Jurnal Nasional Informatika dan Teknologi Jaringan Attribution-NonCommercial 4.0 International*. Some rights reserved Deteksi Penyakit Daun pada Tanaman Padi Menggunakan Algoritma Decision Tree, Random Forest, Naïve Bayes, SVM dan KNN. 5(1). <https://doi.org/10.30743/infotekjar.v5i1.2934>
- [3] Rahman, C. R., Arko, P. S., Ali, M. E., Iqbal Khan, M. A., Apon, S. H., Nowrin, F., & Wasif, A. (2020). Identification and recognition of rice diseases and pests using convolutional neural networks. *Biosystems Engineering*, 194, 112–120. <https://doi.org/10.1016/j.biosystemseng.2020.03.020>
- [4] Alshaibi, A., Al-Ani, M., Al-Azzawi, A., Konev, A., & Shelupanov, A. (2022). The Comparison of Cybersecurity Datasets. In *Data* (Vol. 7, Issue 2). MDPI. <https://doi.org/10.3390/data7020022>
- [5] Mumtaz Ali, M., Zhenfei, W., Weiyan, H., Shabbir, A., Rasheed, A., & Rehman, H. U. (2022). *A State-of-the-Art Technique for Malware Detection Based on Deep Learning in IoT Environment*. <https://doi.org/10.21203/rs.3.rs-2145279/v1>
- [6] Fernando, D. W., Komninos, N., & Chen, T. (2020). A Study on the Evolution of Ransomware Detection Using Machine Learning and Deep Learning Techniques. *IoT*, 1(2), 551–604. <https://doi.org/10.3390/iot1020030>
- [7] Vasan, D., Alazab, M., Wassan, S., Safaei, B., & Zheng, Q. (2020). Image-Based malware classification using ensemble of CNN architectures (IMCEC). *Computers and Security*, 92. <https://doi.org/10.1016/j.cose.2020.101748>
- [8] Pant, D., & Bista, R. (2021, November 26). Image-based Malware Classification using Deep Convolutional Neural Network and Transfer Learning. *ACM*

- [9] Vasan, D., Alazab, M., Wassan, S., Naeem, H., Safaei, B., & Zheng, Q. (2020). IMCFN: Image-based malware classification using fine-tuned convolutional neural network architecture. *Computer Networks*, 171. <https://doi.org/10.1016/j.comnet.2020.107138>
- [10] Algarni, M. D., Alroobaea, R., Almotiri, J., Ullah, S. S., Hussain, S., & Umar, F. (2022). An Efficient Convolutional Neural Network with Transfer Learning for Malware Classification. *Wireless Communications and Mobile Computing*, 2022. <https://doi.org/10.1155/2022/4841741>
- [11] Ahmed, M., Afreen, N., Ahmed, M., Sameer, M., & Ahamed, J. (2023). An inception V3 approach for malware classification using machine learning and transfer learning. *International Journal of Intelligent Networks*, 4, 11–18. <https://doi.org/10.1016/j.ijin.2022.11.005>
- [12] Alzahrani, A. I. A., Ayadi, M., Asiri, M. M., Al-Rasheed, A., & Ksibi, A. (2022). Detecting the Presence of Malware and Identifying the Type of Cyber Attack Using Deep Learning and VGG-16 Techniques. *Electronics (Switzerland)*, 11(22). <https://doi.org/10.3390/electronics11223665>
- [13] Chen, Y. M., Yang, C. H., & Chen, G. C. (2021, January 30). Using Generative Adversarial Networks for Data Augmentation in Android Malware Detection. *2021 IEEE Conference on Dependable and Secure Computing, DSC 2021*. <https://doi.org/10.1109/DSC49826.2021.9346277>
- [14] Marastoni, N., Giacobazzi, R., & Dalla Preda, M. (2021). Data augmentation and transfer learning to classify malware images in a deep learning context. *Journal of Computer Virology and Hacking Techniques*, 17(4), 279–297. <https://doi.org/10.1007/s11416-021-00381-3>
- [15] U. O. Dorj, K. K. Lee, J. Y. Choi, and M. Lee, “The skin cancer classification using deep convolutional neural network,” *Multimed. Tools Appl.*, vol. 77, no. 8, pp. 9909–9924, 2018, doi: <https://doi.org/10.1007/s11042-018-5714-1>.

- [16] Y. Tian, "Artificial Intelligence Image Recognition Method Based on Convolutional Neural Network Algorithm," *IEEE Access*, vol. 8, pp. 125731–125744, 2020, doi: <https://doi.org/10.1109/ACCESS.2020.3006097>.
- [17] H. B. Prajapati, J. P. Shah, and V. K. Dabhi, "Detection and classification of rice plant diseases using image processing techniques," *Intell. Decis. Technol.*, vol. 11, no. 3, pp. 357–373, 2017, doi: <https://doi.org/10.3233/IDT-170301>.
- [18] "Malware Classification Using Data Augmentation with Convolutional Neural Network" oleh M. E. Elsayed, T. S. Abdelghany, dan M. M. Abdelsamea (2021)
- [19] Shijie, J., Ping, W., Peiyi, J., & Siping, H. (n.d.). *Research on Data Augmentation for Image Classification Based on Convolution Neural Networks*. Proc. -2017 Chinese Autom. Congr. CAC 2017, vol. 2017-January, no. 201602118, pp. 4165–4170, 2017, doi: 10.1109/CAC.2017.8243510.
- [20] Gabriela Winarto, E., & Lawi, A. (n.d.). *Konferensi Nasional Ilmu Komputer (KONIK) 2021 Implementasi Arsitektur Inception Resnet-V2 untuk Klasifikasi Kualitas Biji Kakao*.
- [21] Nugraha, P., Komarudin, A., Ramadhan, E., Jenderal, U., Yani, A., & Ji, C. (n.d.). *DETEKSI OBJEK DAN JENIS BURUNG MENGGUNAKAN CONVOLUTIONAL NEURAL NETWORK DENGAN ARSITEKTUR INCEPTION RESNET-V2*. <https://doi.org/10.31949/infotech.v8I2.2889>
- [22] S. Ramesh and D. Vydeki, "Application of machine learning in detection of blast disease in south indian rice crops," *J. Phytol.*, vol. 11, pp. 31–37, 2019, doi: <https://doi.org/10.25081/jp.2019.v11.5476>.
- [23] M. Koklu, I. Cinar, and Y. S. Taspinar, "Classification of rice varieties with deep learning methods," *Dep. Comput. Eng. Selcuk Univ. Konya, Turkey*, vol. 187, 2021, doi: <https://doi.org/10.1016/j.compag.2021.106285>.



UNIVERSITAS
MUHAMMADIYAH
MALANG



FAKULTAS TEKNIK

INFORMATIKA

informatika.umm.ac.id | informatika@umm.ac.id

FORM CEK PLAGIARISME LAPORAN TUGAS AKHIR

Nama Mahasiswa : Jafar Shodiq Djawas
 NIM : 201810370311068
 Judul TA : Implementasi Model Deep Learning InceptionResnet-V2 Untuk Image Classification Pada Malware

Hasil Cek Plagiarisme dengan Turnitin

No.	Komponen Pengecekan	Nilai Maksimal Plagiarisme (%)	Hasil Cek Plagiarisme (%) *
1.	Bab 1 – Pendahuluan	10 %	0 %
2.	Bab 2 – Daftar Pustaka	25 %	13 %
3.	Bab 3 – Analisis dan Perancangan	25 %	4 %
4.	Bab 4 – Implementasi dan Pengujian	15 %	6 %
5.	Bab 5 – Kesimpulan dan Saran	5 %	10 %
6.	Makalah Tugas Akhir	20%	

*) Hasil cek plagiarism diisi oleh pemeriksa (staff TU)

*) Maksimal 5 kali (4 Kali sebelum ujian, 1 kali sesudah ujian)

Mengetahui,

Pemeriksa (Staff TU)



Kampus 1
 Jl. Surodono 1 Malang, Jawa Timur
 P: +62 341 551 253 (runding)
 F: +62 341 400 435

Kampus 2
 Jl. Bawendari Sudarto No. 188 Malang, Jawa Timur
 P: +62 341 551 148 (harung)
 F: +62 341 567 000

Kampus 10
 Jl. Raya Tlogomas No. 248 Malang, Jawa Timur
 P: +62 341 404 318 (harung)
 F: +62 341 403 435
 E: webmaster@umm.ac.id