

**IMPLEMENTASI FORENSIC DISCRIMINATOR BERBASIS
XCEPTIONNET UNTUK DETEKSI DEEFAKE DENGAN
MANIPULASI POST-PROCESSING MANUSIA
SKRIPSI**

Diajukan untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

AMIR NURIL IZZA AL SURUR

22.83.0879

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2026

**IMPLEMENTASI FORENSIC DISCRIMINATOR BERBASIS
XCEPTIONNET UNTUK DETEKSI DEEPFAKE DENGAN
MANIPULASI POST-PROCESSING MANUSIA**
SKRIPSI

untuk memenuhi salah satu syarat mencapai derajat Sarjana
Program Studi Teknik Komputer



disusun oleh

AMIR NURIL IZZA AL SURUR

22.83.0879

Kepada

**FAKULTAS ILMU KOMPUTER
UNIVERSITAS AMIKOM YOGYAKARTA
YOGYAKARTA**

2026

HALAMAN PERSETUJUAN

SKRIPSI

**IMPLEMENTASI FORENSIC DISCRIMINATOR BERBASIS
XCEPTIONNET UNTUK DETEKSI DEEPPAKE DENGAN
MANIPULASI POST-PROCESSING MANUSIA**

yang disusun dan diajukan oleh

Amir Nuril Izza Al Surur

22.83.0879

telah disetujui oleh Dosen Pembimbing Skripsi
pada tanggal 3 Februari 2026

Dosen Pembimbing,


Dr. Dony Arivus, S.S., M.Kom
NIR. 190302128

HALAMAN PENGESAHAN

SKRIPSI

**IMPLEMENTASI FORENSIC DISCRIMINATOR BERBASIS
XCEPTIONNET UNTUK DETEKSI DEEPFAKE DENGAN
MANIPULASI POST-PROCESSING MANUSIA**

yang disusun dan diajukan oleh

Amir Nuril Izza Al Surur

22.83.0879

Telah dipertahankan di depan Dewan Penguji
pada tanggal 18 Februari 2026

Susunan Dewan Penguji

Nama Penguji

Tanda Tangan

Melwin Syafrizal, S.Kom., M.Eng., Ph.D.
NIK. 190302105

Jeki Kuswanto, S.Kom., M.Kom.
NIK. 190302456

Dr. Dony Ariyus, S.S., M.Kom.
NIK. 190302128



Skrripsi ini telah diterima sebagai salah satu persyaratan
untuk memperoleh gelar Sarjana Komputer
Tanggal 18 Februari 2026

DEKAN FAKULTAS ILMU KOMPUTER



Prof. Dr. Kusrini, M.Kom.
NIK. 190302106

HALAMAN PERNYATAAN KEASLIAN SKRIPSI

Yang bertandatangan di bawah ini,

Nama mahasiswa : Amir Nuril Izza Al Surur

NIM : 22.83.0879

Menyatakan bahwa Skripsi dengan judul berikut:
Implementasi Forensic Discriminator Berbasis Xceptionnet Untuk Deteksi Deepfake Dengan Manipulasi Post-Processing Manusia

Dosen Pembimbing : Dr. Donv Arivus, S.S., M.Kom

1. Karya tulis ini adalah benar-benar ASLI dan BELUM PERNAH diajukan untuk mendapatkan gelar akademik, baik di Universitas AMIKOM Yogyakarta maupun di Perguruan Tinggi lainnya.
2. Karya tulis ini merupakan gagasan, rumusan dan penelitian SAYA sendiri, tanpa bantuan pihak lain kecuali arahan dari Dosen Pembimbing.
3. Dalam karya tulis ini tidak terdapat karya atau pendapat orang lain, kecuali secara tertulis dengan jelas dicantumkan sebagai acuan dalam naskah dengan disebutkan nama pengarang dan disebutkan dalam Daftar Pustaka pada karya tulis ini.
4. Perangkat lunak yang digunakan dalam penelitian ini sepenuhnya menjadi tanggung jawab SAYA, bukan tanggung jawab Universitas AMIKOM Yogyakarta.
5. Pernyataan ini SAYA buat dengan sesungguhnya, apabila di kemudian hari terdapat penyimpangan dan ketidakbenaran dalam pernyataan ini, maka SAYA bersedia menerima SANKSI AKADEMIK dengan pencabutan gelar yang sudah diperoleh, serta sanksi lainnya sesuai dengan norma yang berlaku di Perguruan Tinggi.

Yogyakarta, 18 Februari 2026

Yang Menyatakan,



Amir Nuril Izza Al Surur

HALAMAN PERSEMBAHAN

Karya tulis ini saya persembahkan sebagai wujud rasa syukur dan bakti kepada:

1. Kedua orang tua dan keluarga tercinta, Bapak, Ibu, dan Kakak-kakak, yang senantiasa memberikan doa, kasih sayang, serta dukungan moral dan material yang tak terhingga di setiap langkah saya.
2. Diri saya sendiri, yang telah berjuang, bekerja keras, dan tidak pernah menyerah untuk menyelesaikan tanggung jawab pendidikan ini.



KATA PENGANTAR

Puji syukur kehadiran Allah SWT yang telah melimpahkan rahmat dan karunia-Nya, sehingga penulis dapat menyelesaikan skripsi dengan judul **"Implementasi Forensic Discriminator Berbasis XceptionNet untuk Deteksi Deepfake dengan Manipulasi Post-Processing Manusia"**. Skripsi ini disusun sebagai salah satu syarat untuk mencapai derajat Sarjana pada Program Studi Teknik Komputer, Fakultas Ilmu Komputer, Universitas AMIKOM Yogyakarta.

Penulis menyadari bahwa dalam penyusunan skripsi ini tidak lepas dari bimbingan, dukungan, dan bantuan berbagai pihak. Oleh karena itu, pada kesempatan ini penulis ingin menyampaikan ucapan terima kasih yang setulus-tulusnya kepada:

1. Bapak Prof. Dr. M. Suyanto, M.M., selaku Rektor Universitas AMIKOM Yogyakarta.
2. Ibu Prof. Dr. Kusriani, M.Kom., selaku Dekan Fakultas Ilmu Komputer Universitas AMIKOM Yogyakarta .
3. Bapak Dr. Dony Ariyus, S.S., M.Kom., selaku Ketua Program Studi Teknik Komputer Universitas AMIKOM Yogyakarta.
4. Bapak Dr. Dony Ariyus, S.S., M.Kom., selaku Dosen Pembimbing yang telah meluangkan waktu, tenaga, dan pikiran untuk memberikan bimbingan serta arahan selama penyusunan skripsi ini.
5. Bapak/Ibu Dosen Penguji yang telah memberikan masukan dan saran konstruktif demi penyempurnaan skripsi ini.
6. Segenap Dosen dan Staf Universitas AMIKOM Yogyakarta yang telah memberikan bekal ilmu pengetahuan dan bantuan administrasi selama masa perkuliahan.
7. Kedua orang tua dan keluarga tercinta yang senantiasa memberikan doa, kasih sayang, serta dukungan moral dan material yang tak terhingga.
8. Teman-teman seperjuangan di Program Studi Teknik Komputer dan pihak-pihak lain yang tidak dapat penulis sebutkan satu per satu, yang telah memberikan semangat dan bantuan dalam menyelesaikan penelitian ini.

Penulis menyadari bahwa skripsi ini masih jauh dari kesempurnaan. Oleh karena itu, penulis sangat mengharapkan kritik dan saran yang membangun demi perbaikan di masa mendatang. Semoga karya sederhana ini dapat memberikan manfaat bagi pengembangan ilmu pengetahuan, khususnya di bidang keamanan siber dan forensik digital.

Yogyakarta, 22 Desember 2025

Penulis

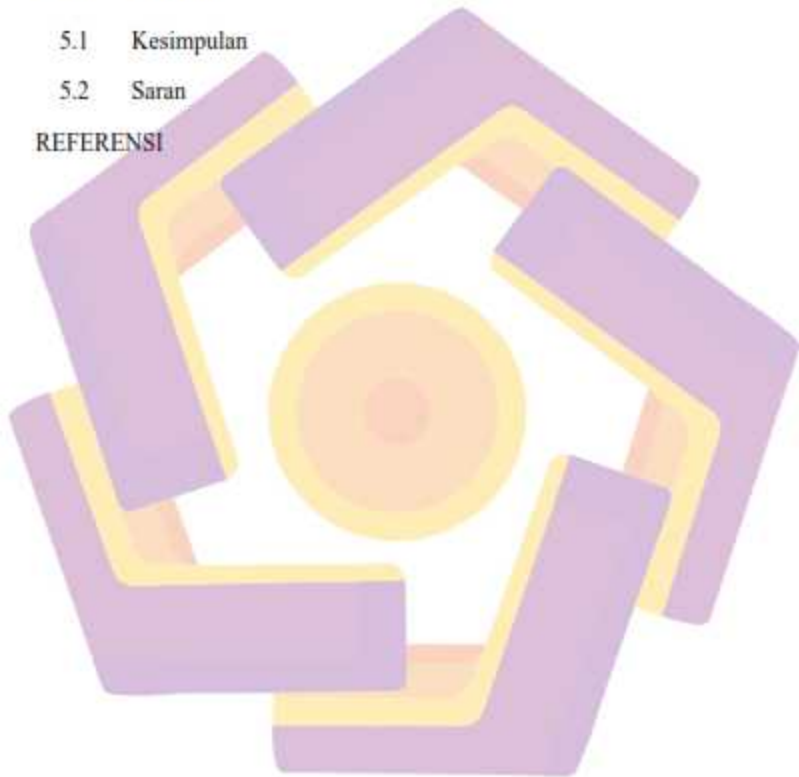


DAFTAR ISI

| | |
|--|------|
| HALAMAN JUDUL | i |
| HALAMAN PERSETUJUAN | ii |
| HALAMAN PENGESAHAN | iii |
| HALAMAN PERNYATAAN KEASLIAN SKRIPSI | iv |
| HALAMAN PERSEMBAHAN | v |
| KATA PENGANTAR | vi |
| DAFTAR ISI | viii |
| DAFTAR TABEL | xi |
| DAFTAR GAMBAR | xii |
| INTISARI | xiv |
| ABSTRACT | xv |
| BAB I PENDAHULUAN | 1 |
| 1.1 Latar Belakang | 1 |
| 1.2 Rumusan Masalah | 2 |
| 1.3 Batasan Masalah | 2 |
| 1.4 Tujuan Penelitian | 3 |
| 1.5 Manfaat Penelitian | 3 |
| 1.6 Sistematika Penulisan | 4 |
| BAB II TINJAUAN PUSTAKA | 6 |
| 2.1 Studi Literatur | 6 |
| 2.2 Dasar Teori | 14 |
| 2.2.1 Deepfake dan Generative Adverarial Networks (GANs) | 14 |
| 2.2.2 Convolutional Neural Network (CNN) | 15 |

| | | |
|------------------------------------|--|-----------|
| 2.2.3 | Arsitektur XceptionNet | 17 |
| 2.2.4 | Forensic Discriminator dan Analisis Tekstur | 19 |
| 2.2.5 | Manipulasi Post-Processing (Smoothing dan Blurring) | 19 |
| 2.2.6 | Pengukuran Kinerja | 20 |
| BAB III METODE PENELITIAN | | 22 |
| 3.1 | Objek Penelitian | 22 |
| 3.2 | Alur Penelitian | 25 |
| 3.3 | Alat dan Bahan | 29 |
| 3.3.1 | Data Penelitian | 29 |
| 3.3.2 | Alat dan Instrumen Penelitian | 31 |
| 3.3.3 | Konfigurasi Hyperparameter | 34 |
| 3.4 | Skenario Penelitian | 35 |
| 3.4.1 | Skenario Pra-pemrosesan Data (<i>Data Preprocessing</i>) | 35 |
| 3.4.2 | Skenario Augmentasi Pertahanan (<i>Defense Augmentation</i>) | 36 |
| 3.4.3 | Skenario Pelatihan Model | 36 |
| 3.4.4 | Skenario Pengujian | 37 |
| BAB IV HASIL DAN PEMBAHASAN | | 38 |
| 4.1 | Implementasi Lingkungan Penelitian | 38 |
| 4.1.1 | Spesifikasi Lingkungan Eksekusi | 38 |
| 4.2 | Hasil Implementasi Manipulasi Post-Processing | 39 |
| 4.3 | Hasil Pelatihan Model (<i>Training Result</i>) | 40 |
| 4.4 | Pengujian dan Evaluasi Kinerja | 42 |
| 4.4.1 | Pengujian Internal | 42 |
| 4.4.2 | Pengujian Eksternal | 47 |
| 4.4.3 | Analisis Penyebab Kegagalan Generalisasi: | 48 |

| | | |
|---------------|--|----|
| 4.5 | Pembahasan dan Analisis | 50 |
| 4.5.1 | Analisis Efektivitas Model pada Manipulasi <i>Post-Processing</i> (Keberhasilan) | 50 |
| 4.5.2 | Analisis Keterbatasan Generalisasi (<i>Domain Shift</i>) | 50 |
| BAB V PENUTUP | | 52 |
| 5.1 | Kesimpulan | 52 |
| 5.2 | Saran | 53 |
| REFERENSI | | 54 |



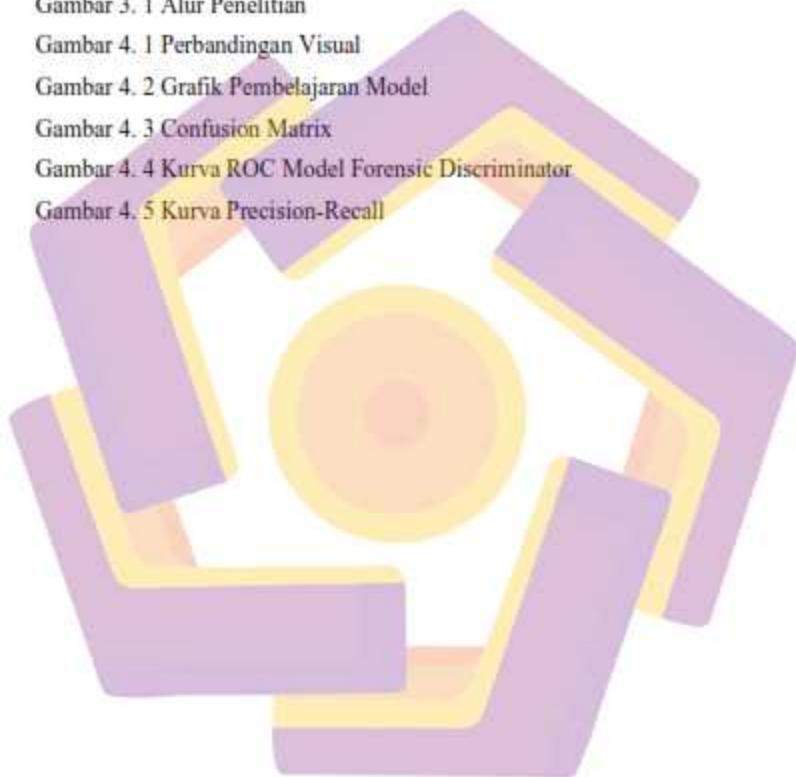
DAFTAR TABEL

| | |
|---|----|
| Tabel 2. 1 Keaslian Penelitian | 10 |
| Tabel 3. 1 Distribusi Dataset Pelatihan | 30 |
| Tabel 3. 2 Instrumen Perangkat Keras | 31 |
| Tabel 3. 3 Instrumen Perangkat Lunak | 32 |
| Tabel 3. 4 Konfigurasi Hyperparameter Model | 34 |
| Tabel 4. 1 Hasil Evaluasi Kinerja Model | 44 |
| Tabel 4. 2 Hasil Pengujian Video Eksternal | 47 |



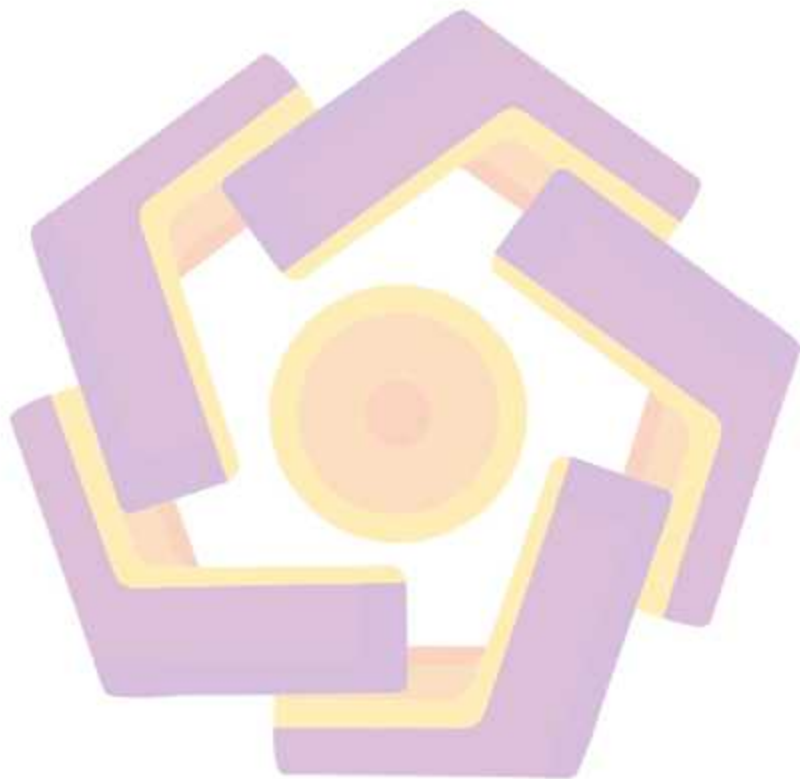
DAFTAR GAMBAR

| | |
|--|----|
| Gambar 2. 1 Arsitektur GANs | 15 |
| Gambar 2. 2 Arsitektur CNN | 16 |
| Gambar 2. 3 Arsitektur XceptionNet | 18 |
| Gambar 3. 1 Alur Penelitian | 26 |
| Gambar 4. 1 Perbandingan Visual | 39 |
| Gambar 4. 2 Grafik Pembelajaran Model | 41 |
| Gambar 4. 3 Confusion Matrix | 43 |
| Gambar 4. 4 Kurva ROC Model Forensic Discriminator | 45 |
| Gambar 4. 5 Kurva Precision-Recall | 46 |



DAFTAR LAMPIRAN

| | |
|--|----|
| Lampiran 1. Tabel Spesifikasi Environment Python | 56 |
| Lampiran 2. Kode Pra-pemrosesan | 57 |
| Lampiran 3. Kode Pembangunan Model (XceptionNet) dan Pelatihan | 58 |



INTISARI

Perkembangan kejahatan siber berbasis *Deepfake* kini semakin kompleks dengan munculnya teknik manipulasi hibrida yang menggabungkan kecerdasan buatan dan penyuntingan manusia (*post-processing*), seperti *smoothing* dan *blurring*. Proses ini menghilangkan artefak visual frekuensi tinggi pada wajah, sehingga video manipulasi menjadi sulit dideteksi oleh model konvensional dan berpotensi menyebarkan disinformasi yang meyakinkan. Penelitian ini bertujuan membangun sistem deteksi *Forensic Discriminator* menggunakan arsitektur *Convolutional Neural Network (CNN) XceptionNet* yang diperkuat dengan strategi *Defense Augmentation*. Metode yang diterapkan meliputi pelatihan model menggunakan 39.924 *frame* citra wajah dari gabungan dataset *FaceForensics++*, *Celeb-DF*, dan *DFDC*. Untuk meningkatkan ketahanan model, 50% data latih kelas *fake* diberikan perlakuan khusus berupa filter *Gaussian*, *Median*, dan *Bilateral* guna mensimulasikan penyamaran jejak digital. Hasil pengujian validasi internal menunjukkan performa yang sangat tinggi dengan Akurasi 98,38%, *Recall* 97,65%, dan *AUC* 0,9993, yang membuktikan bahwa model mampu mendeteksi manipulasi halus sekalipun tekstur wajah telah disamarkan. Meskipun terdapat penurunan performa pada data eksternal akibat *domain shift*, penelitian ini memberikan kontribusi signifikan bagi praktisi keamanan siber dalam menyediakan metode deteksi yang tangguh terhadap serangan anti-forensik visual.

Kata kunci: *Deepfake*, *XceptionNet*, *Forensic Discriminator*, *Post-Processing*, *Defense Augmentation*.

ABSTRACT

The development of cybercrime based on Deepfake is becoming increasingly complex with the emergence of hybrid manipulation techniques that combine artificial intelligence and human editing (post-processing), such as smoothing and blurring. This process removes high-frequency visual artifacts on the face, making manipulated videos difficult for conventional models to detect and potentially spreading convincing disinformation. This study aims to build a Forensic Discriminator detection system using the XceptionNet Convolutional Neural Network (CNN) architecture enhanced with a Defense Augmentation strategy. The applied method involves training the model using 39,924 face image frames from a combined dataset of FaceForensics++, Celeb-DF, and DFDC. To improve model robustness, 50% of the fake class training data was given special treatment in the form of Gaussian, Median, and Bilateral filters to simulate digital trace masking. Internal validation test results showed superior performance with 98.38% Accuracy, 97.65% Recall, and 0.9993 AUC, proving that the model is capable of detecting subtle manipulations even when face textures have been disguised. Although there was a decrease in performance on external data due to domain shift, this research makes a significant contribution to cybersecurity practitioners by providing a detection method that is robust against visual anti-forensic attacks.

Keyword: *Deepfake, XceptionNet, Forensic Discriminator, Post-Processing, Defense Augmentation.*