BAB I
PENDAHULUAN

Setiap hari, banyak gambar dan video diunggah kedalam Internet, tetapi keaslian dari gambar dan video tersebut tidak bisa dipastikan kebenarannya. Penyebaran gambar palsu melalui Internet dapat menyebabkan keresahanpolitik dan sosial yang tidak diinginkan. Jadi, sangat penting untukmemvalidasi keaslian gambar digital. Saat ini, mudahnya orang-orangmengedit dan bertukar wajah menggunakan aplikasi berbasis AI yang bisadigunakan hampir setiap orang, yang secara luas dikenal sebagai DeepFakes.Semakin lama, kemunculan deepfake semakin meresahkan dunia. Jumlah konten manipulasi yang diciptakan dengan teknologi kecerdasan buatan ini begitu cepat berlipat ganda di dunia maya. Penyebabnya, berbagai perangkatlunak yang bisa digunakan untuk membuat deepfake, baik video ataupun
audio, tumbuh subur.

Menurut penelitian perusahaan asal Belanda yang berfokus padapenciptaan teknologi pendeteksi deepfake, Deeptrace, dalam kurun waktu tujuh bulan, jumlah video deepfake meningkat dua kali lipat. Pada Desember 2018, jumlah video deepfake hanya sebanyak 7.964 video. Pada Juli 2019, jumlah video deepfake sudah mencapai 14.678 video.

Menurut pendiri Deeptrace, Giorgio Patrini, meningkatnya jumlah video deepfake ini didukung oleh pertumbuhan komodifikasi berbagai perangkatserta layanan yang memungkinkan semua orang membuat video deepfake.“Adanya berbagai perangkat dan layanan ini memperkecil halangan bagiseseorang yang bukan ahli untuk menciptakan video deepfake,” kata Patrini. Yang lebih memprihatinkan, menurut penelitian ini, sebanyak 96 persen dari jumlah video deepfake yang tersebar di internet itu bermuatanpornografi. Video-video yang diunggah dalam empat situs khusus videodeepfake porno pun sudah ditonton hingga lebih dari 134 juta kali. Seluruhvideo yang ditemukan di situs-situs tersebut menyasar perempuan di mana 99

persen di antaranya berisi selebritas serta musisi perempuan dan sisanya berisi pekerja industri media perempuan.

Di YouTube, tren video deepfake sedikit berbeda. Menurut penelitian ini, sebanyak 61 persen video deepfake di YouTube yang tidak memuat konten pornografi menyasar laki-laki. Namun, sebagian besar targetnya tetap selebritas dan musisi, yakni sebanyak 81 persen. Sementara sisanya menyasar politikus, pekerja industri media, serta pengusaha.

Inilah faktor yang mengerikan dari machine learning yang dimiliki AI, karena mampu meningkatkan kemampuannya dengan luar biasa dan dilakukan hanya dalam waktu singkat. Namun, sayangnya kecanggihan metode ini dimanfaatkan oleh oknum yang tidak bertanggung jawab.

Bila masalah Deepfakes ini tidak segera ditangani dengan baik maka akantimbul bahaya yang sangat meresahkan masyarakat, bila itu menyerang seleberitis tentu akan membuat namanya menjadi tercemar dan bisa mendapakan hukuman dari sesuatu yang sebenarnya tidak ia lakukan, dan apabila deepfake menyerang para politikus tentu akan mencoreng namabaiknya dan akan timbul persaingan politik yang tidak sehat sehingga berpotensi membuat lawan politik atau masyarakat menjadi terpecah belah.

Tentunya potensi bahaya yang terjadi sedini mungkin harus bisa ditanganiagar tidak menimbulkan permasalahan yang lebih kompleks dimasa yang akan mendatang. Dengan kualitas Deepfakes yang kian hari kian meningkat tentu kinerja metode deteksi perlu ditingkatkan pula. Inspirasinya adalah bahwa apa yang telah rusak oleh AI dapat diperbaiki oleh AI juga.

Metode untuk klasifikasi yang popular saat ini ialah CNN (*Convolutional Neural Network),* Sampai saat ini, metode deteksi Deep Fakes mengandalkan untuk mempelajari artefak atau inkonsistensi intrinsik untuk algoritma sintesis, misalnya, kurangnya kedipan mata yang realistis dan profil warna yang tidak cocok pada video deepfake. Pendekatan klasifikasi berbasis jaringan saraf juga telah digunakan untuk membedakan secara langsung citra nyata dari Deep Fakes. Namun jika menggunakan metode tersebut kita

membutuhkan dataset yang banyak sehingga mempengaruhi performa saat melakukan pelatihan.

Metode ID-Reveal merupakan metode yang mempelajari fitur wajah temporal, spesifik tentang bagaimana seseorang bergerak saat berbicara, melalui pembelajaran metrik yang digabungkan dengan strategi pelatihan permusuhan. Selain itu Deepfake yang menggunakan Dynamic Face Augmentation Face-Cutout, metode augmentasi data untuk melatih Convolutional Neural Networks (CNN), guna meningkatkan deteksi DeepFake. Dalam metode ini, gambar pelatihan dengan berbagai oklusi dihasilkan secara dinamis menggunakan informasi landmark wajah terlepas dari orientasinya.

Dari sini penulis tertarik untuk mengkombinasikan metode ID-Reveal danFace Augmenetation kami mendefinisikan jaringan saraf dalam saraf convolutional untuk gambar multi-saluran *(RGB)*, kernel yang berbeda diterapkan ke setiap saluran, dan output ditambahkan bersama-sama berdasarkan piksel.

Dengan metode tersebut jadi tidak lagi memerlukan video deepfake yangbanyak untuk dataset. Hal tersebut tentu akan lebih ringan untuk digunakan dalam computer dengan spek standar.

Berdasarkan tinjauan dan uraian permasalahan diatas maka peneliti mengangkat penelitian tesis ini dengan judul "Kombinasi *Dynamic Face Augmentation* dan *ID-Reveal* untuk klasifikasi *Deepfake Detection* menggunakan metode *Convolutional Neural Network*".

1. 2 Identifikasi Masalah

Berdasarkan latar belakang penelitian diatas, terdapat beberapa permasalah yang diidentifikasi, yaitu bahayanya penyalahgunaan deepfake, urgensi untuk deepfake detection dan bagaimana untuk meningkatkan algoritma untuk *deepfake detection*.

1. 3 Batasan Masalah

Berdasarkan identifikasi rumusan masalah yang telah dilakukan, agar penelitian tetap terarah kepada tujuan akhir penelitian, maka disimpulkan beberapa scope atau batasan masalah antara lain:

a. Penelitian ini bertujuan untuk mendeteksi gambar atau video fake atau real menggunakan *Convolutional Neural Network* (CNN) yang berdasarkan posisi wajah pada foto/video.
b. Analisa algoritma yang berdasarkan adalah akurasi, kecepatan, dan kesederhanaan dalam mengimpelmentasikannya.
c. Arsitektur Convolutional Neural Network yang akan digunakan adalah Pytorch versi 1.7.
d. Simulasi akan dilakukan dalam bahasa pemrograman Paython 3.

1. 4 Rumusan Masalah

Berdasarkan identifikasi masalah yang telah dirumuskan tersebut, dapat disimpulkan beberapa rumusan masalah, antara lain:

a. Bagaimana mendeteksi gambar dan video fake atau real menggunakan *Convolutional Neural Network* (CNN)?
b. Bagaimana performa *Convolutional Neural Network* (CNN) untuk mendeteksi *deepfake*?

1. 5 Tujuan Penelitian

Tujuan dalam penelitian ini adalah untuk mendapatkan algoritma deep learning mendeteksi gambar dan video fake atau real dan menganalisa performa algoritma tersebut dari akurasi, dan kecepatan waktu dalam melatih modelnya.

1. 6 Manfaat Penelitian Penelitian

Manfaat yang ingin dicapai melalui penelitian ini adalah:

1. Bagi Penulis

a. Memenuhi salah satu syarat kelulusan Strata Dua (S2) Program Studi Ilmu Komputer pada Universitas Esa Unggul.
b. Penerapan ilmu pengetahuan yang diperoleh pada saat kuliah, melatih diri untuk berpikir secara kritis dalam pemecahan masalah, dan memberikan pengalaman belajar yang baru secara praktek di lapangan
c. Untuk membantu pihak kepolisian atau terkait dalam memberantas berita bohong yang dibuat dengan video/gambar palsu.

2. Bagi Pembaca
   a. Memberikan gambaran serta penyelesaian masalah dalam menghadapi masalah deepfake yang makin meresahkan.
   b. Memberikan gambaran mengenai metode *Convolutional Neural Network* (CNN) dalam melakukan klasifikasi *deepfake detection*

1. 7 Kontribusi Penelitian

Adapun kontribusi penelitian yang dilakukan berfokus pada pengembangan arsitektur *deep learning* dan deteksi gambar dan video *deepfake*