

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi kecerdasan buatan (*Artificial intelligence/AI*), khususnya pada bidang *deep learning*, telah membawa kemajuan pesat dalam pengolahan citra dan video digital. Salah satu implikasi dari kemajuan tersebut adalah munculnya teknologi *Deepfake*, yaitu teknik manipulasi citra atau video yang memanfaatkan jaringan saraf tiruan untuk menghasilkan wajah manusia yang tampak sangat *realistis*. Teknologi *Deepfake* mampu meniru ekspresi wajah, gerakan bibir, serta karakteristik visual seseorang sehingga sulit dibedakan dari wajah asli oleh pengamatan manusia secara langsung (Korshunov & Marcel, 2018).

Meskipun teknologi *Deepfake* memiliki potensi positif dalam bidang hiburan dan industri kreatif, penyalahgunaannya menimbulkan ancaman serius terhadap keamanan informasi dan kepercayaan publik terhadap konten digital. *Deepfake* dapat dimanfaatkan untuk penipuan identitas, pemalsuan video tokoh publik, penyebaran informasi palsu (*misinformation*), serta tindak kejahatan siber lainnya. Rossler *et al.*, (2019) menyatakan bahwa kualitas manipulasi wajah pada *Deepfake* modern telah mencapai tingkat yang sangat realistis sehingga pendeteksian secara manual menjadi semakin sulit.

Fenomena *Deepfake* juga mulai menjadi perhatian di Indonesia. Penelitian yang dilakukan oleh Jurnal Pendidikan Tambusai membahas bahwa teknologi *Deepfake* berpotensi mengancam keamanan komunikasi digital karena kemampuannya memanipulasi konten visual secara meyakinkan, sehingga masyarakat sulit membedakan antara informasi yang asli dan palsu (Tambun *et al.*, 2024). Kondisi ini menunjukkan pentingnya pengembangan sistem pendeteksian *Deepfake* yang mampu bekerja secara otomatis dan akurat.

Dalam konteks *face recognition*, penelitian sebelumnya menunjukkan bahwa penggunaan kombinasi beberapa metode *edge detection* seperti *Robert*, *Prewitt*, *Sobel*, dan *Canny* yang dikombinasikan dengan *Canberra distance* mampu meningkatkan akurasi pengenalan wajah secara signifikan. Metode ini lebih cepat

dan lebih akurat dibandingkan menggunakan satu teknik *edge detection* saja, serta lebih efisien dalam penggunaan memori (Intan *et al.*, 2023)

Berbagai penelitian telah mengembangkan pendekatan berbasis *deep learning* untuk mendeteksi *Deepfake*. Salah satu arsitektur *Convolutional Neural Network (CNN)* yang banyak digunakan adalah *Xception*, yang diperkenalkan oleh (Chollet, 2017). Arsitektur *Xception* memanfaatkan *depthwise separable convolution* untuk meningkatkan efisiensi komputasi dan kemampuan ekstraksi fitur. Beberapa penelitian menunjukkan bahwa *Xception* memiliki performa yang baik dalam mendeteksi artefak visual khas pada citra *Deepfake* (Rossler *et al.*, 2019).

Namun, proses klasifikasi *Deepfake* tidak dapat dilakukan secara optimal tanpa menentukan area wajah yang relevan pada citra atau video. Oleh karena itu, diperlukan tahap deteksi wajah sebagai langkah awal. Algoritma *YOLO (You Only Look Once)* merupakan salah satu metode *object detection* yang mampu mendeteksi objek secara cepat dan akurat dalam satu tahap pemrosesan (*single-stage detector*). *YOLO* banyak digunakan dalam berbagai aplikasi *real-time* termasuk deteksi wajah karena kecepatan dan tingkat akurasi yang tinggi (Redmon *et al.*, 2016).

YOLOv11 merupakan versi terbaru dari algoritma *YOLO* yang dirilis pada tahun 2024. Model ini memperkenalkan sejumlah peningkatan dibandingkan versi sebelumnya, antara lain penerapan *multi scale prediction* untuk meningkatkan deteksi objek dengan ukuran yang bervariasi, sistem *anchor* yang diperbarui, dan juga penggunaan *backbone network* yang lebih efisien dalam mengekstraksi visual. Perkembangan arsitektur *YOLO* dari generasi awal hingga versi terbaru menunjukkan peningkatan signifikan dalam performa deteksi objek, baik dari sisi kecepatan maupun akurasi (Ilyana *et al.*, 2025).

Penelitian di Indonesia juga menunjukkan keefektifan metode *deep learning* untuk deteksi dan klasifikasi wajah. (Sugianto *et al.*, 2022) berhasil mengimplementasikan *YOLOv3* untuk sistem pengenalan wajah pada presensi dengan hasil yang akurat. Penelitian tersebut menunjukkan bahwa *YOLO* efektif digunakan dalam deteksi wajah secara *real-time* dan dapat dijadikan tahap awal sebelum proses klasifikasi citra dilakukan. Selain itu, metode CNN terbukti mampu

melakukan klasifikasi citra wajah dengan tingkat akurasi yang baik. (Zarkasi *et al.*, 2022) dalam penelitiannya tentang klasifikasi gambar bergerak pada pengenalan wajah menggunakan *CNN* menunjukkan bahwa metode ini efektif dalam mengidentifikasi wajah dengan akurasi tinggi dalam berbagai penelitian nasional. Sejalan dengan hal tersebut, (Gunawan *et al.*, 2023) membuktikan bahwa integrasi metode *YOLO* dan *CNN* mampu menghasilkan sistem deteksi dan klasifikasi berbasis citra dengan performa yang sangat baik, meskipun objek berada dalam kondisi bergerak. Temuan ini memperkuat bahwa pendekatan kombinasi deteksi dan klasifikasi *deep learning* dapat diadaptasi pada bidang lain, termasuk pendeteksian *Deepfake* wajah.

Berdasarkan beberapa penelitian terdahulu tersebut, penelitian ini mengusulkan sistem pendeteksian *Deepfake* wajah menggunakan metode *YOLO* sebagai pendeteksi wajah dan *Xception* sebagai pengklasifikasi wajah asli dan *Deepfake* berbasis *Tensorflow*. *Tensorflow* dipilih sebagai *framework* pengembangan karena mendukung implementasi *deep learning* secara fleksibel dan efisien. Sistem ini diharapkan mampu memberikan solusi dalam mendeteksi konten *Deepfake* wajah secara otomatis serta berkontribusi dalam meningkatkan keamanan konten digital.

Urgensi penelitian ini didasari dengan semakin maraknya penyalahgunaan teknologi *Deepfake* yang dapat menimbulkan berbagai dampak negatif, seperti penyebaran hoaks, kejahatan digital, serta pelanggaran privasi dan keamanan informasi. Ketiadaan sistem pendeteksian yang akurat dan otomatis menyebabkan konten *Deepfake* semakin sulit dikenali dan dibedakan dari citra wajah asli oleh penglihatan manusia. Oleh sebab itu, penelitian ini menjadi penting untuk mengembangkan sistem pendeteksian *Deepfake* wajah yang efektif dan aplikatif, guna mendukung peningkatan keamanan serta kepercayaan terhadap konten digital.

1.2 Rumusan Masalah

Berdasarkan ulasan latar belakang di atas, rumusan masalah dalam penelitian ini diuraikan sebagai berikut:

1. Bagaimana cara mendeteksi *Deepfake* pada wajah manusia secara akurat dan efisien?
2. Apa kelebihan dan keterbatasan metode *Xception* dan *YOLOv11* dalam pendeteksian *Deepfake*?
3. Bagaimana implementasi sistem berbasis *Tensorflow* untuk aplikasi praktis?

1.3 Tujuan Penelitian

Berdasarkan ulasan rumusan masalah di atas, rumusan masalah dalam penelitian ini diuraikan sebagai berikut:

1. Mengembangkan sistem pendeteksian *Deepfake* wajah menggunakan *Xception* dan *YOLOv11* berbasis *Tensorflow*.
2. Mengevaluasi performa sistem terhadap dataset *Deepfake* dan non *Deepfake*.
3. Menganalisis efektivitas kombinasi metode untuk deteksi *real-time*.

1.4 Ruang Lingkup dan Penelitian

Agar penelitian ini lebih fokus dan terarah, maka ditetapkan batasan masalah sebagai berikut:

1. Penelitian ini fokus pada deteksi *Deepfake* wajah pada citra dan video, tidak mencakup *Deepfake* audio atau teks.
2. Dataset yang digunakan adalah dataset *FaceForensics++* yang merupakan dataset publik standar untuk penelitian *Deepfake*.
3. Metode deteksi wajah yang digunakan adalah *YOLOv11*, dan metode klasifikasi yang digunakan adalah *Xception*.
4. *Framework* yang digunakan untuk implementasi adalah *Tensorflow* versi 2.21.0.
5. Evaluasi sistem dilakukan menggunakan metrik akurasi, presisi, *recall*, dan *F1-score*.
6. Penelitian ini tidak membahas metode pembuatan *Deepfake*, melainkan fokus pada pendeteksiannya.
7. Sistem yang dikembangkan di uji coba pada kondisi laboratorium dengan spesifikasi hardware yang telah ditentukan.

1.5 Manfaat Penelitian

Penelitian ini diharapkan dapat memberikan manfaat sebagai berikut:

1. Menambah kajian dan pemahaman dalam bidang *computer vision* dan *Deep learning*, khususnya terkait deteksi *Deepfake* pada citra dan video wajah.
2. Menjadi bahan rujukan bagi penelitian selanjutnya yang membahas pendeteksian manipulasi citra dan video menggunakan metode *Deep learning*.
3. Menghasilkan sistem yang dapat digunakan untuk mendeteksi konten *Deepfake* wajah secara otomatis.
4. Membantu mengurangi penyebaran konten visual palsu dengan meningkatkan proses verifikasi keaslian citra dan video.
5. Memberikan kemudahan bagi individu maupun instansi dalam memastikan keaslian konten digital.
6. Dapat dimanfaatkan sebagai alat bantu pada platform media sosial atau aplikasi keamanan digital.