

BAB I

PENDAHULUAN

1.1 Latar Belakang

Perkembangan teknologi informasi dan komunikasi yang pesat ternyata menjadikan dampak yang serius pada berbagai aspek kehidupan manusia. Di era digital ini, Artificial Intelligence semakin memainkan peran yang kritis dalam menghasilkan, mengedit, manipulasi, serta menyebarkan konten dalam bentuk teks, gambar, atau video. Salah satu fenomena yang perlu menjadi bahan kajian dalam beberapa tahun terakhir adalah deepfake, teknik manipulasi media berbasis deep learning yang memungkinkan pembuatan video palsu pada tingkat kualitas tinggi.

Deepfake adalah produk dari penerapan teknologi Jaringan Pertaruhan Generatif (GAN) atau algoritma yang berbasiskan pada jaringan saraf dalam. Teknologi ini memberikan kemampuan untuk mengganti wajah atau suara seseorang dalam video dengan hasil yang tampak sangat meyakinkan. Meskipun pada awalnya teknologi ini dirancang untuk tujuan yang positif seperti dalam sektor film, hiburan, dan pendidikan, dalam praktiknya, deepfake sering disalahgunakan untuk menyebarluaskan informasi palsu, pornografi tanpa persetujuan, pemerasan, dan juga propaganda politik. Ini menjadikan deepfake sebuah ancaman serius bagi keamanan informasi, privasi individu, dan kepercayaan publik terhadap konten digital.

Di Indonesia, laju perkembangan teknologi AI semakin cepat, bersamaan dengan bertumbuhnya penggunaan media sosial sebagai sumber utama

informasi bagi masyarakat. Situasi ini memberikan peluang besar bagi oknum yang tidak bertanggung jawab untuk menyebarkan video yang telah dimanipulasi, bertujuan untuk menyesatkan pandangan publik atau merusak nama baik seseorang. Kementerian Komunikasi dan Informatika (Kominfo) telah beberapa kali mengangkat isu munculnya konten deepfake yang viral di berbagai platform digital, yang seringkali sulit untuk dibedakan oleh masyarakat awam dari video yang asli. Ini menunjukkan bahwa penting untuk mengembangkan teknologi deteksi video deepfake, sehingga publik bisa membedakan antara konten yang nyata dan yang telah dimanipulasi.

Salah satu metode yang umum diterapkan dalam mengidentifikasi video deepfake adalah dengan menggunakan algoritma Convolutional Neural Network (CNN). CNN adalah bagian dari Deep Learning yang sangat mumpuni dalam mengidentifikasi pola visual baik pada gambar maupun video. Kemampuan untuk mengenali detail seperti perbedaan pencahayaan wajah, ketidaksesuaian pergerakan bibir, atau distorsi pada tekstur kulit membuat CNN bisa dilatih untuk secara otomatis mendeteksi video yang telah dimanipulasi. Berbagai studi menunjukkan bahwa model CNN seperti XceptionNet, ResNet, dan EfficientNet mampu mencapai akurasi tinggi dalam mendeteksi deepfake, baik menggunakan dataset publik maupun video hasil modifikasi baru. Dengan penerapan algoritma CNN, sebuah sistem deteksi deepfake dapat dikembangkan untuk menganalisis setiap frame video dan memberikan hasil klasifikasi mengenai keaslian video tersebut. Proses ini bisa diintegrasikan ke dalam aplikasi berbasis komputer yang

mudah untuk digunakan, baik untuk tujuan akademik, penelitian, maupun pendidikan masyarakat. Dengan keberadaan sistem ini, diharapkan dapat membantu masyarakat dan institusi terkait dalam memverifikasi keaslian video yang beredar dengan cepat, efisien, dan akurat.

Studi ini menjadi signifikan dan krusial untuk dilakukan di lingkungan Universitas Darma Persada, sebagai wujud nyata penerapan teknologi informasi untuk mengatasi tantangan digital yang kian rumit. Selain memberikan sumbangsih akademis dalam perkembangan algoritma pendeteksian video yang menggunakan CNN, penelitian ini juga menawarkan manfaat praktis dalam merangsang keterampilan digital dan kesadaran mengenai keamanan data di kalangan mahasiswa serta masyarakat umum. Oleh karena itu, penelitian yang berjudul “Penerapan Algoritma Convolutional Neural Network (CNN) untuk Deteksi Video Deepfake di Universitas Darma Persada” diharapkan dapat menciptakan sebuah sistem deteksi yang terpercaya dan berkontribusi pada usaha pencegahan penyebaran informasi yang tidak benar di zaman digital ini. Kajian ini juga merupakan langkah strategis dalam mendukung peningkatan keamanan siber serta integritas informasi di wilayah Indonesia.

1.2 Rumusan Masalah

Bagaimana cara menerapkan algoritma Convolutional Neural Network (CNN) untuk membangun sistem pendeteksi video deepfake yang mampu membantu Universitas Darma Persada dalam mengidentifikasi keaslian video yang beredar dan mencegah penyebaran konten manipulatif yang dapat merusak citra

serta reputasi kampus maupun civitas akademika?

1.3 Batasan Masalah

- a. Data yang digunakan berupa video wajah yang bersumber dari dataset publik (Kaggle (DFD manipulated sequence)).
- b. Fokus penelitian terbatas pada deteksi video deepfake berbasis wajah manusia, tanpa membahas manipulasi audio atau teks.
- c. Algoritma yang digunakan adalah Convolutional Neural Network (CNN) tanpa kombinasi dengan model lain seperti RNN atau Transformer.
- d. Sistem hanya dibangun dalam bentuk prototype aplikasi desktop atau berbasis web lokal untuk keperluan penelitian di Universitas Darma Persada.
- e. Pengujian dilakukan pada data uji yang dibatasi oleh ukuran dan format tertentu (misalnya *.mp4* dengan resolusi standar).

1.4 Tujuan Penelitian

- a. Mengembangkan model Convolutional Neural Network (CNN) yang mampu mendeteksi video deepfake dengan tingkat akurasi tinggi.
- b. Membangun sistem deteksi otomatis yang dapat mengklasifikasikan video menjadi kategori asli atau manipulasi (deepfake).
- c. Mengevaluasi kinerja model CNN berdasarkan metrik seperti akurasi, presisi, recall, dan F1-score.
- d. Menyediakan prototype sistem yang dapat digunakan sebagai alat bantu edukasi dan penelitian dalam bidang keamanan informasi digital.

1.5 Manfaat Penelitian

1 Manfaat Teoritis

- 1) Menambah wawasan dan literatur dalam bidang kecerdasan buatan dan pengolahan citra digital, khususnya pada penerapan algoritma CNN untuk deteksi manipulasi video.
- 2) Memberikan kontribusi terhadap penelitian Deep Learning dalam konteks forensik digital dan keamanan siber.
- 3) Menjadi acuan bagi penelitian lanjutan dalam pengembangan model yang lebih kompleks seperti 3D CNN atau spatiotemporal networks.

2 Manfaat Praktis

- 1) Menghasilkan sistem pendeteksi deepfake yang dapat digunakan oleh mahasiswa, dosen, dan masyarakat umum untuk menguji keaslian video.
- 2) Mendukung upaya edukasi literasi digital di lingkungan Universitas Darma Persada agar civitas akademika lebih kritis terhadap konten digital.
- 3) Menjadi langkah awal dalam pengembangan teknologi keamanan informasi berbasis AI di institusi pendidikan Indonesia.

1.6 Lokasi Penelitian

Penelitian ini berfokus pada lingkungan Universitas Darma Persada sebagai objek penelitian, khususnya pada permasalahan potensi penyebaran video deepfake di kalangan mahasiswa, dosen, dan civitas akademika. Objek ini dipilih karena kampus merupakan lingkungan yang aktif dalam pertukaran informasi digital melalui media sosial dan platform komunikasi daring, sehingga rentan

terhadap penyalahgunaan teknologi manipulasi video.

Sistem deteksi video deepfake yang dikembangkan dalam penelitian ini tidak dibangun menggunakan perangkat keras atau laboratorium kampus, melainkan dibuat secara mandiri menggunakan perangkat pribadi dan sumber daya daring. Penelitian ini difokuskan pada pengembangan website pendeteksi deepfake yang dirancang untuk membantu mahasiswa dan pihak kampus dalam memverifikasi keaslian video yang beredar di lingkungan akademik. Dengan demikian, Universitas Darma Persada dalam penelitian ini berperan sebagai objek penerapan dan simulasi kasus, bukan sebagai lokasi teknis pelaksanaan eksperimen. Hasil dari penelitian ini diharapkan dapat menjadi sarana edukatif dan preventif bagi civitas akademika dalam menghadapi potensi penyebaran video manipulatif yang dapat merugikan individu maupun lembaga.

1.7 Pengguna Sistem

- a. Mahasiswa — untuk memeriksa keaslian video yang beredar di lingkungan kampus, terutama jika ada indikasi video yang merugikan reputasi pribadi atau kelompok.
- b. Dosen dan Staf Akademik — untuk memastikan bahwa materi atau video yang dikaitkan dengan civitas akademika bukan hasil manipulasi yang menyesatkan.
- c. Pihak Administrasi Kampus / Tim Humas — sebagai alat bantu awal dalam menangani insiden deepfake yang dapat mempengaruhi citra institusi.

- d. Peneliti & Mahasiswa Penelitian — untuk keperluan studi lebih lanjut, eksperimen model, dan pengembangan deteksi multimodal di lingkungan akademik.

1.8 Metode Penelitian

Penelitian ini menggunakan pendekatan eksperimental dengan penerapan algoritma ConvolutionalNeuralNetwork(CNN).

Tahapan penelitian meliputi:

1. Pengumpulan Data – mengambil video asli dan deepfake dari dataset publik dan simulasi kampus.
2. Pemahaman Data – menganalisis struktur video dan ciri khas deepfake.
3. Pengolahan Data – melakukan ekstraksi frame, preprocessing, dan pelatihan model CNN.
4. Evaluasi Model – mengukur performa model dengan akurasi, presisi, recall, dan F1-score.
5. Implementasi Sistem – membangun website pendeteksi video deepfake berbasis Python dan MySQL.

1.9 Studi Pustaka

Berbagai penelitian terdahulu menjadi dasar bagi penelitian ini, di antaranya:

1. Korshunov & Marcel (2018) menggunakan CNN untuk mendeteksi artefak spasial dan temporal pada video deepfake.
2. XceptionNet (2019) dalam kompetisi DeepFake Detection Challenge (DFDC) mencapai hasil akurasi tinggi pada dataset besar.
3. Penelitian lain menunjukkan bahwa preprocessing wajah dan transfer learning dapat meningkatkan performa model CNN dalam mengenali deepfake.

1.10 Metode Pemahaman Data

Tahapan ini bertujuan untuk memahami karakteristik dataset video yang digunakan.

Langkah-langkahnya:

1. Mengidentifikasi jenis video asli dan video deepfake.
2. Melakukan frame extraction untuk mengubah video menjadi kumpulan gambar.
3. Melakukan observasi visual terhadap pola khas deepfake seperti distorsi wajah, pencahayaan tidak alami, dan ekspresi yang tidak sinkron.

1.11 Metode Pengolahan Data

Proses pengolahan data dilakukan dengan langkah-langkah berikut:

1. Ekstraksi Frame: memecah video menjadi gambar per frame.
2. Preprocessing: meliputi deteksi wajah, cropping, normalisasi ukuran, dan augmentasi.
3. Pelatihan Model CNN: menggunakan dataset hasil preprocessing.
4. Klasifikasi: model CNN mengkategorikan video sebagai *asli* atau *deepfake*.

1.12 Metode Evaluasi Model

Evaluasi model dilakukan untuk mengukur tingkat keberhasilan sistem.

Metrik yang digunakan antara lain:

1. Akurasi (Accuracy): proporsi prediksi benar.
2. Presisi (Precision): ketepatan model mendeteksi deepfake.
3. Recall: kemampuan model menangkap semua data deepfake.
4. F1-score: keseimbangan antara presisi dan recall.

1.13 Metode Pengumpulan Data

Data diperoleh dari:

1. Dataset publik, seperti **DeepFake Detection Dataset (DFD)** dan **FaceForensics++**.
2. Video simulasi kampus, yaitu video yang dibuat untuk meniru kondisi penyebaran konten manipulatif di lingkungan akademik.

Seluruh data yang digunakan dijamin tidak melanggar privasi dan telah melalui proses izin dan etika penelitian yang berlaku di Universitas Darma Persada.

