

# BAB 1

## PENDAHULUAN

### 1.1 Latar Belakang Masalah

*Deepfake* adalah teknologi berbasis *deep learning* yang digunakan untuk memanipulasi gambar, audio, atau video dengan sangat meyakinkan, sehingga sulit dibedakan dari konten asli. Teknologi ini bekerja dengan memanfaatkan jaringan saraf tiruan seperti Generative Adversarial Networks (GANs) dan Autoencoders untuk menghasilkan konten sintetik yang tampak realistis [1]. Berdasarkan data dari Security Hero, jumlah video *deepfake* tercatat setidaknya 95.820 video *deepfake* tersebar secara global, yang menunjukkan peningkatan sebesar 550% dari tahun 2019 sampai tahun 2023, dengan mayoritas digunakan dalam konten eksploitasi non-konsensual [2]. Metode deteksi konvensional seperti analisis inkohereni visual dan analisis metadata sering kali tidak cukup efektif dalam mengidentifikasi video *deepfake*, terutama dengan semakin canggihnya teknik manipulasi seperti *face swapping* dan *head puppetry*. Akibatnya, teknologi ini berpotensi disalahgunakan untuk penyebaran disinformasi, manipulasi opini publik, dan peretasan identitas digital [3].

Berbagai pendekatan telah dikembangkan untuk mendeteksi *deepfake*, mulai dari teknik berbasis analisis visual hingga model berbasis kecerdasan buatan. Salah satu pendekatan yang semakin populer adalah pemanfaatan Neural Network, seperti Convolutional Neural Network (CNN) dan Recurrent Neural Network (RNN) yang terbukti mampu mengenali pola-pola tidak wajar dalam video hasil manipulasi [4]. Selain itu, beberapa penelitian juga mengusulkan pendekatan berbasis deteksi artefak digital atau analisis spektrum frekuensi wajah yang bertujuan untuk membedakan wajah asli dan hasil sintesis berdasarkan perbedaan tekstur atau pola frekuensi yang tidak kasat mata [5].

Penelitian sebelumnya telah mengembangkan berbagai pendekatan dalam deteksi *deepfake*. Jeevidha (2023) menggunakan kombinasi dataset Celeb-DF dan FaceForensics++ untuk melatih model ResNet-50 dan LSTM mereka yang memungkinkan deteksi lebih akurat dan adaptif terhadap berbagai teknik manipulasi yang semakin berkembang [6]. Selain itu, Patil (2024) mengembangkan pendekatan *hybrid* CNN-RNN-LSTM yang mengintegrasikan fitur spasial dan temporal, sehingga meningkatkan akurasi dalam mendeteksi *deepfake* berbasis

anomali ekspresi wajah [7]. Namun, mayoritas penelitian masih bergantung pada dataset yang memiliki keterbatasan dalam representasi kondisi dunia nyata, seperti FaceForensics++ dan Celeb-DF [8]. Oleh karena itu, penelitian Sohan (2024) mengusulkan penggunaan *dataset* ForgeryNet, yang mencakup manipulasi lebih kompleks, termasuk pemalsuan berbasis GAN, pertukaran wajah tingkat lanjut, serta manipulasi ekspresi dan gerakan wajah [8]. Dengan penggunaan *dataset* ForgeryNet, model deteksi diharapkan dapat lebih adaptif terhadap ancaman *deepfake* terbaru dan meningkatkan ketahanan terhadap berbagai teknik manipulasi.

Dalam penelitian ini, metode yang diusulkan menggabungkan ResNet-50 dan LSTM untuk mendeteksi video *deepfake*. ResNet-50 digunakan karena efektif dalam mengekstraksi fitur visual dari setiap frame, seperti tekstur dan pencahayaan, yang penting untuk mendeteksi manipulasi visual. Sementara itu, LSTM mampu menangkap pola temporal antar frame, seperti perubahan ekspresi dan gerakan wajah [9]. Penggabungan keduanya diperlukan karena ResNet-50 saja tidak mampu memahami urutan waktu, dan LSTM membutuhkan vektor fitur yang dihasilkan dari proses ekstraksi ResNet-50. Oleh karena itu, kombinasi ResNet-50 dan LSTM memungkinkan deteksi *deepfake* yang lebih komprehensif [6]. Perbedaan penelitian ini dengan penelitian sebelumnya adalah jumlah *hyperparameter* yang dieksplorasi lebih banyak, yaitu 10 *hyperparameter*, dibandingkan hanya 5 *hyperparameter* pada penelitian sebelumnya, sehingga memungkinkan pencarian konfigurasi model yang lebih optimal. Selain itu, ForgeryNet dipilih sebagai *dataset* karena menawarkan variasi manipulasi yang lebih kaya dibandingkan *dataset* sebelumnya, seperti FaceForensics++. *Dataset* ini mencakup beragam teknik *deepfake*, kondisi pencahayaan, ekspresi wajah, dan latar belakang, sehingga memberikan tantangan yang lebih realistis bagi model. Dengan menggunakan ForgeryNet, diharapkan model deteksi dapat dilatih untuk lebih adaptif dan akurat dalam menghadapi variasi manipulasi yang mungkin muncul dalam skenario dunia nyata.

## 1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, rumusan masalah pada penelitian ini adalah:

- Bagaimana implementasi ResNet-50 dan LSTM dalam mengembangkan model untuk deteksi video *deepfake* ?

- Berapa tingkat akurasi model deteksi berbasis ResNet-50 dan LSTM dalam mengidentifikasi video *deepfake* ?

### 1.3 Batasan Permasalahan

Untuk menjaga fokus penelitian, beberapa pembatasan permasalahan yang diterapkan adalah:

- Penelitian ini berfokus pada proses pelatihan dan evaluasi model deteksi *deepfake* tanpa mencakup implementasi sistem secara keseluruhan seperti pengembangan antarmuka pengguna.
- Data video *deepfake* yang dianalisis dalam penelitian ini dibatasi sebanyak 6000 video yang diambil dari *dataset* ForgeryNet.

### 1.4 Tujuan Penelitian

Tujuan yang ingin dicapai dari penelitian ini untuk menjawab masalah yang terdapat pada rumusan masalah di atas antara lain:

- Mengimplementasikan ResNet-50 dan LSTM dalam mengembangkan model untuk deteksi video *deepfake*.
- Mengukur tingkat akurasi dari model deteksi berbasis ResNet-50 dan LSTM dalam mengidentifikasi video *deepfake*.

### 1.5 Manfaat Penelitian

Pada bagian ini diuraikan manfaat yang akan diperoleh dari penelitian ini diantara lain:

- Menyediakan model deteksi untuk mengidentifikasi video asli atau *deepfake* berdasarkan *image* wajah.
- Membantu proses pencegahan penipuan dan disinformasi yang dapat timbul akibat adanya konten manipulatif yang menggunakan *deepfake* sebagai perantaranya.

## 1.6 Sistematika Penulisan

Berisikan uraian singkat mengenai struktur isi penulisan laporan penelitian, dimulai dari Pendahuluan hingga Simpulan dan Saran.

Sistematika penulisan laporan adalah sebagai berikut:

- Bab 1 PENDAHULUAN  
Bab ini terdiri dari enam bagian, yaitu latar belakang masalah, rumusan masalah, batasan permasalahan, tujuan penelitian, manfaat penelitian, dan sistematika penulisan.
- Bab 2 LANDASAN TEORI  
Bab ini membahas kajian pustaka yang berkaitan dengan penelitian, termasuk teori-teori dasar mengenai *deepfake*, model deteksi berbasis ResNext dan LSTM, serta penelitian terdahulu yang relevan.
- Bab 3 METODOLOGI PENELITIAN  
Bab ini menjelaskan metodologi penelitian yang digunakan, meliputi desain penelitian, tahapan penelitian, pemrosesan data, dan teknik evaluasi model deteksi *deepfake*.
- Bab 4 HASIL DAN DISKUSI  
Bab ini menyajikan hasil penelitian dan analisisnya, termasuk pengujian model deteksi *deepfake*, hasil metrik performa seperti *accuracy*, *precision*, *recall*, dan *F1-score*, serta pembahasan terhadap temuan penelitian.
- Bab 5 KESIMPULAN DAN SARAN  
Bab ini berisi kesimpulan dari hasil penelitian serta saran untuk pengembangan penelitian lebih lanjut di masa depan.

U N I V E R S I T A S  
M U L T I M E D I A  
N U S A N T A R A