BAB I
PENDAHULUAN

1.1 Latar Belakang

Pendeteksian pada wajah merupakan langkah penting dalam banyak pembuatan apliasi,seperti facial expression, face recognition maupun emotion recognition. Pendeteksian pada wajah dilakukan untuk mengidentifikasi keberadaan wajah dalam video, dan ketika wajah terdeteksi, posisinya akan ditandai di dalam frame (Megawan & Lestari, 2020).

Namun,terdapat kelemahan dalam mengenali wajah dalam konteks serangan pemalsuan identitas. Dengan memanfaatkan sebuah sistem pengenalan saja sistem belum tentu mampu membedakan antara wajah sebenarnya atau palsu seperti menggunakan video maupun foto dari pengguna. Dengan memanfaatkan kelemahan ini seseorang dapat melakukan spoofing pada sistem.Selain itu,untuk mendapatkan wajah seseorang biasanya lebih mudah di dapatkan dibandingkan dengan biometrik lainnya, seperti sidik jari di karenakan wajah seseorang bisa dengan mudah di dapatkan melalui jejaringan sosial (Budiarto Hadiprakoso 2021)

Serangan spoofing pada pengenalan wajah dapat dikategorikan menjadi dua jenis serangan: statis dan dinamis. Serangan statis merupakan serangan yang menggunakan objek yang tidak mengalami pergerakan atau tidak berubah selama proses identifikasi wajah seperti foto wajah seseorang. Sedangkan pada serangan yang dinamis mengacu pada serangan yang dapat bergerak seperti video dari wajah seseorang (Buana, 2021).

Penempatan atribut wajah berupa mata,hidung, alis dagu dan bibir merupakan pendekatan yang paling umum di lakukan dalam pengenalan wajah dengan menggabungkan hubungan antara atribut tersebut (Alwendi & Masriadi, 2021).

Banyak algoritma yang telah yang telah diusulkan dalam melakukan pendeteksian wajah melalui foto atau video Salah satunya dengan menggunakan algoritma Convolutional Neural Network (CNN). Convolutional Neural Network merupakan deep learning yang dirancang untuk memproses data 2 dimensi dengan struktur jaringan yang mendalam. Jaringan yang dimaksud adalah jaringan syaraf tiruan yang

digunakan untuk pengolahan citra, khususnya dalam hal klasifikasi dan pengenalan objek (Fadlil et al., 2022).

Selain CNN, Haar Cascade Classifier juga merupakan algoritma yang sering digunakan dalam melakukan pendeteksi objek pada sebuah image. Keunggulan dari metode ini terletak pada kecepatan komputasinya yang tinggi hal dikarenakan pada dalam metode ini bukan bergantung pada setip nilai piksel melainkan pada jumlah piksel pada sebuah image (Septyanto et al., 2019).

1.2 Identifikasi Masalah

Berdasarkan uraian latar belakang masalah yang telah disampaikan, berikut adalah identifikasi permasalahan yang dituliskan pada penelitian ini:

1. Sistem pengenalan wajah rentan terhadap serangan spoofing hal ini karenakan di sistem tidak dapat membedakan antara wajah asli dan wajah tiruan seperti foto maupun video
2. Data wajah seseorang dapat dengan mudah diakses dari media sosial, membuat wajah menjadi lebih rentan terhadap serangan spoofing dibandingkan biometrik lainnya seperti sidik jari
3. Berbagai metode dan algoritma seperti CNN dan Haar Cascade yag digunakan untuk mendeteksi wajah. CNN mampu mempelajari pola kompleks dan efektif dalam deteksi spoofing, sedangkan Haar Cascade lebih cepat dalam komputasi meski kurang kompleks.

1.3 Batasan Masalah

1. Fokus pada masalah serangan spoofing dalam pengenalan wajah.
2. Fokus pada metode Convolutional Neural Network (CNN) dan Haar Cascade dalam deteksi wajah dan identifikasi serangan spoofing.
3. Penelitian ini dibatasi pada serangan spoofing statis (2D dan 3D) dan dinamis.

1.4 Rumusan masalah

Berdasarkan identifikasi masalah di atas, rumusan masalah dalam penelitian ini adalah sebagai berikut:

1. Dari kedua metode tersebut manakah yang paling tepat dalam hal akurasi untuk di gunakan dalam mendeteksi serangan spoofing?
2. Apa saja kelemahan dalam sistem pengenalan wajah yang dapat menyebabkan

kerentanan terhadap serangan spoofing?

1.5 Tujuan Penelitian

Tujuan dari penelitian ini adalah mengimlemtasikan Convolutional Neural Network (CNN) dan Haar Cascade Classifier sebagai perbandingan metode yang tepat untuk menghindari serangan spoofing pada wajah, serta mengidentifikasi kelemahan utama dalam sistem pengenalan wajah ini yang menyebabkan kerentanan terhadap serangan tersebut.

1.6 Manfaat Penlitian

Manfaat dari penelitian yang akan di lakukan ini adalah sebagai berikut

1.6.1 Manfaat Teoritis

1. Diharapkan hasil penelitian ini dapat memperluas wawasan maupun pengetahuan tentang metode dan algoritma yang efektif dalam deteksi wajah dalam mengidentifikasi spoofing.
2. Diharapkan hasil penilitan ini dapat menjadi bahan referensi bagi penelitian selanjutnya terkait deteksi wajah dan keamanan sistem pengenalan wajah.

1.6.2 Manfaat Praktis.

1. Dalam bidang pendidikan, teknologi ini dapat digunakan untuk membantu memantau kehadiran dan partisipasi siswa secara otomatis
2. Dalam bidang keamanan,teknologi ini dapat diteapkan untuk keamanan rumah dengan memastikan hanya penghuni yang diizinkan dapat mengakses rumah, mengurangi risiko akses oleh pihak yang tidak berwenang