BAB I

PENDAHULUAN

1.1. Latar Belakang

Sejak zaman dahulu hingga sekarang, tanda tangan banyak digunakan untuk mengautentikasi dan mengotorisasi transaksi elektronik, namun hal ini juga rentan terhadap pemalsuan. Ketika masyarakat semakin bergantung pada interaksi digital, ancaman pemalsuan menimbulkan risiko besar bagi individu, organisasi, dan pemerintah. Maka dari itu, pengembangan teknologi untuk mengetahui pemalsuan tanda tangan digital sangat penting untuk memahami metodologi yang digunakan oleh pelaku kejahatan dan mengembangkan mekanisme keamanan yang kuat. Terutama sejak adanya pandemic Covid-19, penelitian ini juga memberikan landasan untuk memajukan protokol kriptografi menggunakan kepintaran buatan yang berperan penting dalam kebutuhan autentifikasi tanda tangan ketika situasi terbatas akan kehadiran secara fisik oleh penandatangan[1][2].

Penelitian pemalsuan tanda tangan digital adalah bidang penelitian keamanan siber yang penting. Dengan memahami tanda tanda yang tidak normal dari tanda tangan tiruan, mengembangkan mekanisme keamanan yang kuat, dapat membantu melindungi integritas dan kerahasiaan jejak digital, sehingga menumbuhkan kepercayaan dalam mengautentifikasi berkas penting, hingga memastikan keberlanjutan ekonomi digital modern. Selain itu, penelitian di bidang ini tidak hanya membantu dalam mengidentifikasi dan mengurangi pemalsuan tanda tangan digital tetapi juga memberikan landasan bagi kemajuan protokol kriptografi dan algoritma tanda tangan digital yang dapat dibedakan oleh biometrik[3].

Upaya penelitian dalam bidang ini telah memberikan kontribusi terhadap pemahaman tentang ancaman dan kerentanan yang terkait dengan tanda tangan digital, sehingga memungkinkan pengembangan mekanisme keamanan yang lebih kuat untuk melindungi transaksi dan data digital. Dalam mengembangan mekanisme keamanan, *deep learning* dan *machine learning* sangat dibutuhkan. Kecerdasan buatan tingkat lanjut dapat digunakan untuk menerapkan cara kerja

yang mengajarkan komputer untuk membuat ramalan dan belajar dari data tanpa diprogram secara eksplisit. *Deep learning* adalah jenis cara fungsi utama mesin yang menggunakan jaringan tiruan untuk belajar dari data[4]. Sebuah model yang memberikan fungsi berhubungan pada lapisan data terhubung dapat membentuk sistem sederhana yang dapat melatih data terus menerus[5]. Kumpulan data yang melatihan jaringan sistem dengan berbagai layer ekstrasi untuk mempelajari pola kompleks dalam data dengan parameter yang mengumpulkan banyak kemungkinan hasil optimal dan tepat[6]. Untuk melakukan hal ini, jaringan sistem dilatih pada kumpulan data besar yang berisi tanda tangan asli dan palsu. Jaringan sistem belajar untuk secara otomatis menilai fitur-fitur dari gambar tanda tangan yang serupa dengan bentuk, pembuatan guratan, dan tekanan pena[7].

Seperti yang dikatakan dalam artikel jurnal sebelumnya, jaringan Convolutional Neural Networks (CNN) dan Algoritma Genetika memiliki keunggulan dalam melatih model verifikasi tanda tangan offlineHal ini dapat dioptimalkan menggunakan algoritma genetika untuk optimasi hipermetrik arsitektur CNN. Penelitian ini bertujuan untuk menyoroti fitur tanda tangan yang efektif dan memverifikasi apakah sistem dapat secara otomatis memverifikasi tanda tangan asli dan mendeteksi pemalsuan yang terampil. Hasil eksperimen menunjukkan bahwa akurasi verifikasi meningkat ketika pengklasifikasi berbasis fitur digabungkan. Model yang dibangun untuk memvalidasi tanda tangan melalui transfer fungsi pembelajaran dan aktivasi untuk tiga model CNN yang berbeda (VGG16, VGG19, dan ResNet50) dengan penambahan beberapa parameter untuk setiap model, pelatihan[8]. Selain itu, beberapa teknik digunakan untuk pengenalan tanda tangan dalam penelitian yang disebutkan. Beberapa tekniknya antara lain fitur berbasis bentuk, HMM kiri ke kanan, fitur berorientasi guratan, analisis komponen utama, dan arsitektur CNN VGG16[1]. Makalah lainnya juga mengusulkan metode yang menggunakan prediksi yang akurat untuk membedakan tanda tangan asli dan palsu. Metode penelitian ini menggunakan bahasa pemrograman Python dengan *library* TensorFlow untuk verifikasi dan Convolutional Neural Networks (CNN) untuk ekstraksi fitur. Tantangan verifikasi tanda tangan yaitu PERBANDINGAN METODE TRANSFER LEARNING DALAM DETEKSI PEMALSUAN TANDA

TANGAN DIGITAL yang variabilitas pada tanda tangan seseorang, dan dua metode verifikasi: online dan offline merupakan bagian penting pemrosesan gambar dalam verifikasi tanda tangan dan penggunaan jaringan sistem *deep learning* untuk meniru cara kerja otak manusia. [9]. ada beberapa metode dan pendekatan yang disebutkan dalam konten untuk verifikasi tanda tangan offline dan deteksi pemalsuan, seperti usulan kumpulan fitur berdasarkan properti keliling tanda tangan, *local binary pattern (LBP), global feature descriptor (GIST), and convolutional neural network (CNN).* Saran penelitian kedepannya diperlukan akses ke lebih banyak sumber daya, seperti kumpulan data yang lebih besar dengan lebih banyak contoh tanda tangan, kinerja yang lebih baik dapat dicapai dalam penelitian ini[10], [11].

Penelitian ini bertujuan untuk memperkuat infrastruktur keamanan tanda tangan digital dengan menjadikannya lebih tahan terhadap ancaman yang muncul dan pergeseran teknologi. Hal ini akan melibatkan pemeriksaan komprehensif terhadap algoritme yang ada untuk mengidentifikasi kerentanan dan memanfaatkan teknik kriptografi mutakhir untuk mengembangkan algoritme tanda tangan digital yang lebih aman dan tangguh. Dengan menyelaraskan algoritma dengan *deep learning,* penelitian ini bertujuan untuk membandingkan model Convolutional Neural Network dengan *transfer learning* untuk deteksi pemalsuan gambar digital signature, diharapkan dapat berkontribusi pada kemajuan ilmu kriptografi tetapi juga memberdayakan individu, organisasi, dan pemerintah untuk menavigasi dunia yang semakin digital dengan terpercaya dan aman.

1.2. Rumusan Masalah

Terdapat beberapa rumusan masalah dalam penelitian terkait sebagai berikut:

1. Bagaimana pendekatan *transfer learning* dengan arsitektur model VGG16, EfficientNetB0, dan ConvNext terhadap model deteksi pemalsuan berdasarkan tanda tangan?
2. Bagaimana meningkatkan akurasi kinerja model deteksi pemalsuan tanda tangan yang optimal?
3. Bagaimana hasil akurasi data train dan validasi yang diberikan pada penelitian terkait ?

1.3. Tujuan Penelitian

Terdapat beberapa tujuan dalam penelitian terkait sebagai berikut:

1. Merancang model dengan perancangan arsitektur *transfer learning* yang dapat mendeteksi pemalsuan tanda tangan palsu.
2. Merancang model deteksi pemalsuan gambar berdasarkan pemalsuan tanda tangan menggunakan optimasi *hyperparameter* dengan arsitektur model untuk melihat apakah model yang dihasilkan lebih baik daripada penelitian terdahulu.
3. Menganalisa hasil akurasi data *training* dan validasi yang diberikan pada penelitian terkait.

1.4.Urgensi Penelitian

Penelitian terhadap pemalsuan tanda tangan sangat diperlukan karena masyarakat semakin mengandalkan tanda tangan digital dalam hal-hal penting dan identifikasi dokumen, sehingga risiko penipuan tanda tangan semakin meningkat. Dampak negatif dari pemalsuan tanda tangan mencakup penipuan finansial, litigasi, pencurian identitas, dan pelanggaran privasi, yang semuanya dapat menimbulkan konsekuensi pemalsuan bukti identitas. Untuk mengatasi masalah yang berkembang ini secara efektif, keakuratan model deteksi palsu harus ditingkatkan setinggi mungkin. Model yang sangat akurat ini memastikan bahwa tanda tangan yang sah tidak secara tidak sengaja ditandai sebagai pemalsuan, menjaga integritas transaksi dan dokumen yang sah, serta secara efektif mendeteksi tanda tangan palsu untuk mencegah aktivitas ilegal. Ketepatan ini sangat penting untuk melindungi individu dan organisasi dari konsekuensi finansial dan hukum yang signifikan akibat pemalsuan tanda tangan di dunia yang semakin digital.

1.5. Luaran Penelitian

Hasil penelitian dapat dipublikasikan dalam berbagai bentuk, termasuk jurnal ilmiah dan konferensi ilmiah. Hasil penelitian yang dipublikasikan dalam

jurnal ilmiah biasanya mengikuti proses peer review yang ketat sesuai dengan akreditasi jurnal. Penelitian ini kemungkinan akan memiliki analisis yang lebih mendalam dan rinci, serta pemahaman yang lebih lengkap tentang topik tersebut. Jurnal ilmiah yang dituju untuk publikasi adalah Jurnal Nasional Teknik Elektro Dan Teknologi Informasi dengan akreditasi Sinta 2 yang menyesuaikan kriteria durasi MBKM penelitian ini.

1.6.Manfaat Penelitian

Berikut merupakan manfaat dari penelitian ini seperti:

1. Merancang model dengan akurasi optimal untuk mendeteksi pemalsuan tanda tangan berdasarkan kemiripan garis dan ciri-ciri tanda tangan berbasis digital untuk mengidentifikasi apakah tanda tangan tersebut telah dipalsukan atau asli.
2. Membantu mengoptimalkan akurasi model deteksi tanda tangan yang telah dipalsukan sehingga penyalahgunaan otoritas berbasis tanda tangan dapat dihindari.
3. Membantu melindungi integritas jejak autentifikasi individu di dunia digital.