

BAB II

TINJAUAN LITERATUR

2.1 Penelitian Terkait

Tinjauan pustaka dapat berisi tentang kerangka *konseptual* maupun landasan teori yang menjadi penguat ataupun pijakan ketika melakukan penelitian. Berikut merupakan beberapa referensi artikel yang berkaitan dengan identifikasi keaslian tanda tangan.

Penelitian oleh Simon Simarmata tahun 2023 yang membahas deteksi akurasi tanda tangan menggunakan metode Support Vector Machine (SVM) dan Zernike Moment pada SMA Harapan Bangsa. Data dikumpulkan dari 78 responden yang membubuhkan tanda tangan mereka, kemudian diproses melalui tahapan praproses seperti grayscale, binerisasi, cropping, dan ekstraksi fitur. Sistem dirancang dengan menggunakan MATLAB untuk mengklasifikasi keaslian tanda tangan berdasarkan dataset training dan testing. Hasil penelitian menunjukkan bahwa kombinasi metode SVM dan Zernike Moment mampu meningkatkan tingkat akurasi pengenalan tanda tangan hingga mencapai 97,93%, sehingga lebih efektif dalam mencegah pemalsuan tanda tangan. Penelitian ini menegaskan bahwa kualitas citra dan pemilihan fitur sangat berpengaruh terhadap tingkat akurasi verifikasi tanda tangan (Simarmata, 2023).

Penelitian selanjutnya oleh Dechy Deswita tahun 2022, meneliti identifikasi tanda tangan menggunakan Convolutional Neural Network (CNN). Penelitian ini melibatkan 150 sampel tanda tangan dari 15 responden, dengan data dibagi 80%

untuk pelatihan dan 20% untuk pengujian. Citra tanda tangan diproses melalui tahapan resizing, augmentasi, noise reduction, normalisasi, kemudian diekstraksi fitur oleh CNN melalui lapisan konvolusi, pooling, hingga fully connected layer. Hasil pengujian menunjukkan bahwa model CNN mampu mengenali tanda tangan dengan akurasi sangat tinggi, mencapai 97%, dengan precision 0.98 dan recall 0.97. Temuan ini membuktikan bahwa CNN sangat efektif dan andal dalam identifikasi tanda tangan serta berpotensi besar untuk digunakan dalam sistem keamanan dan autentikasi otomatis (Indriani.S *et al.*, 2024).

Penelitian selanjutnya oleh Jefri Sianipar tahun 2022 yang membahas analisis keaslian tanda tangan menggunakan algoritma RIPEMD160 berbasis hash kriptografi. Metode ini menghasilkan nilai hash unik dari citra tanda tangan digital sehingga dapat membedakan tanda tangan asli dan palsu. Penelitian dilakukan dengan mengubah citra tanda tangan menjadi bilangan biner, lalu diproses untuk memperoleh hash 160-bit sebagai identitas unik. Implementasi sistem dibuat menggunakan Visual Basic 2010, mencakup proses input tanda tangan, pembuatan hash, penyimpanan, hingga validasi keaslian. Hasil menunjukkan bahwa RIPEMD160 efektif dalam mendeteksi perubahan sekecil apapun pada citra tanda tangan, sehingga mampu mencegah pemalsuan dokumen digital secara efisien (Sianipar, 2022).

Penelitian selanjutnya membahas identifikasi tanda tangan menggunakan Metode Jaringan Syaraf Tiruan (JST) Backpropagation. Penelitian dilakukan dengan mengolah citra tanda tangan melalui tahapan preprocessing, ekstraksi ciri, pelatihan jaringan, dan pengujian. Data tanda tangan diubah menjadi pola biner

yang kemudian dilatih menggunakan algoritma backpropagation hingga bobot jaringan optimal tercapai. Hasil penelitian menunjukkan bahwa metode ini mampu mengenali tanda tangan dengan tingkat akurasi cukup baik, meskipun performa sangat dipengaruhi oleh jumlah data latih, parameter jaringan, serta kualitas citra masukan. JST Backpropagation dinilai efektif sebagai dasar pengembangan sistem autentikasi tanda tangan digital (Sandy, Widodo and Sari, 2018).

Penelitian yang terakhir membahas pengenalan tanda tangan dengan kombinasi pengolahan citra dan Support Vector Machine (SVM). Penelitian ini menggunakan 300 citra tanda tangan dosen pembimbing skripsi yang diproses melalui preprocessing, kemudian dilakukan ekstraksi ciri menggunakan Filter Gabor, HSV (Hue Saturation Value), dan GLCM (Gray Level Co-occurrence Matrix). Hasil ekstraksi kemudian diklasifikasikan menggunakan metode SVM. Dari pengujian menggunakan Confusion Matrix Multi Class, sistem mampu mencapai tingkat akurasi yang sangat tinggi yaitu 99,43%. Temuan ini menunjukkan bahwa kombinasi metode ekstraksi ciri dengan SVM sangat efektif dalam mengidentifikasi keaslian tanda tangan dan berpotensi diaplikasikan dalam sistem validasi dokumen akademik (Pujianto, Lestari and Septiani, 2021).

Dari beberapa penelitian tersebut dapat disimpulkan bahwa, penelitian ini menawarkan pengembangan melalui penggunaan Hu Moments sebagai metode ekstraksi fitur. Keunggulan Hu Moments adalah sifatnya yang invarian terhadap translasi, rotasi, dan skala, sehingga lebih robust dibandingkan metode lain dalam menghadapi variasi posisi, ukuran, dan orientasi tanda tangan. Selain itu, Hu Moments memiliki kompleksitas perhitungan yang lebih ringan dibanding CNN

atau kombinasi multi-metode, sehingga dapat diimplementasikan secara efisien dalam aplikasi praktis. Dengan mengombinasikan Hu Moments dengan algoritma klasifikasi yang tepat (misalnya SVM atau ensemble classifier), sistem yang Anda usulkan berpotensi mencapai akurasi tinggi sekaligus tetap ringan dijalankan pada perangkat dengan spesifikasi menengah.

2.2 Pengolahan Citra Digital

Pengolahan citra adalah suatu bidang dalam ilmu komputer dan teknik yang berfokus pada proses transformasi, analisis, dan interpretasi citra (gambar digital) menggunakan algoritma komputasional untuk memperoleh informasi yang bermakna, meningkatkan kualitas visual, atau mempersiapkan data untuk tugas-tugas automasi selanjutnya (G. W, Toyib and Wijaya, 2025). Secara mendasar, pengolahan citra mengambil data citra sebagai masukan (input) dan menghasilkan baik citra yang telah dimodifikasi maupun sekumpulan karakteristik atau keputusan berdasarkan konten citra tersebut (Supiyandi Supiyandi *et al.*, 2024).

Dalam konteks penelitian deteksi pemalsuan tanda tangan digital, pengolahan citra merupakan fondasi dan proses kritis yang mentransformasi citra tanda tangan mentah menjadi data terstruktur yang siap dianalisis secara komputasional untuk mengidentifikasi keaslian. Proses ini dimulai dari akuisisi citra, yang kemudian melalui serangkaian tahap pra-pemrosesan. Tahap pra-pemrosesan, meliputi konversi ke skala keabuan, penghalusan (smoothing) untuk mengurangi noise, dan peningkatan kontras, bertujuan untuk memperoleh citra yang bersih dan seragam, sehingga memudahkan tahap analisis berikutnya. Selanjutnya, dilakukan segmentasi untuk memisahkan objek tanda tangan dari latar

belakangnya. Setelah citra biner atau grayscale yang terpisah diperoleh, proses kunci yaitu ekstraksi fitur dilakukan (Mayangky *et al.*, 2021). Di sinilah HU Moments berperan sebagai fitur deskriptor bentuk yang sangat efektif. Berdasarkan momen geometris yang dinormalisasi, HU Moments mampu mengekstraksi tujuh nilai numerik yang merepresentasikan karakteristik bentuk global tanda tangan dengan sifat invarian terhadap translasi, penskalaan, dan rotasi (Sebatubun and Haryawan, 2024). Dengan demikian, fitur-fitur ini menangkap esensi unik dari gaya tanda tangan asli yang sangat sulit untuk ditiru secara sempurna oleh pemalsu.



Gambar 2.1 Alur pemrosesan dalam pengolahan citra

Gambar tersebut menampilkan alur proses pengolahan citra digital. Proses dimulai dari tahap Citra Masukan (Image Acquisition) yang menggambarkan proses pengambilan gambar menggunakan perangkat seperti kamera atau drone sebagai sumber data awal. Tahap berikutnya adalah Pra-Pemrosesan (Pre-Processing), yang bertujuan untuk meningkatkan kualitas citra melalui proses seperti perbaikan kontras, reduksi noise, atau konversi ke grayscale agar citra lebih siap dianalisis. Selanjutnya masuk ke tahap Segmentasi dan Ekstraksi Fitur, di mana objek penting pada citra dipisahkan dari latar belakang dan ciri-ciri khususnya diambil untuk direpresentasikan dalam bentuk data numerik. Tahap keempat adalah Klasifikasi dan Pengenalan (Classification & Recognition) yang memanfaatkan metode kecerdasan buatan atau pembelajaran mesin untuk mengidentifikasi dan mengelompokkan objek berdasarkan fitur yang telah diekstraksi. Terakhir, proses menghasilkan Hasil Akhir (Result Output) berupa informasi, keputusan, atau visualisasi hasil analisis yang ditampilkan pada layar sebagai keluaran sistem. Secara keseluruhan, gambar tersebut menjelaskan tahapan sistematis dalam pengolahan citra mulai dari input hingga menghasilkan output yang bermakna.

2.3 Preprocessing

Preprocessing atau pra-pemrosesan dalam pengolahan citra merupakan tahap kritis yang bertujuan untuk mempersiapkan citra mentah agar siap untuk dianalisis lebih lanjut, dengan meningkatkan kualitas dan keseragamannya. Tahap ini umumnya mencakup beberapa proses fundamental (Lapendy *et al.*, 2024). Pertama, grayscaling atau konversi ke skala keabuan dilakukan untuk menyederhanakan citra dengan mengubah piksel berwarna menjadi nilai intensitas

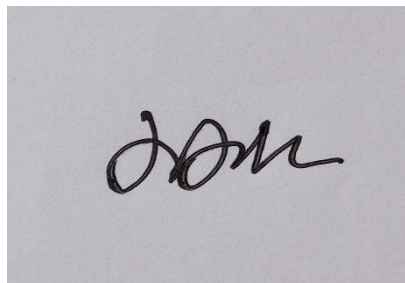
abu-abu, yang mengurangi kompleksitas komputasi dan memfokuskan analisis pada pola intensitas daripada informasi warna (Novanni *et al.*, 2025). Selanjutnya, binerisasi diterapkan untuk mengubah citra grayscale menjadi citra hitam-putih dengan memilih suatu ambang batas (threshold), sehingga objek utama (seperti tanda tangan) dapat dipisahkan secara jelas dari latar belakang, memudahkan proses segmentasi dan ekstraksi fitur bentuk (Mar'ah *et al.*, 2025). Tahap normalisasi ukuran kemudian dilakukan untuk menstandarisasi dimensi semua citra, baik dengan resizing, cropping, atau padding, guna menjamin konsistensi geometris yang sangat penting untuk perhitungan fitur yang akurat dan komparatif antar sampel (Muhammad *et al.*, 2024). Terakhir, penghilangan noise melalui teknik seperti filtering (misalnya Gaussian filter atau median filter) berperan untuk membersihkan citra dari gangguan-gangguan seperti titik-titik acak atau goresan halus yang muncul selama akuisisi, sehingga menghasilkan citra yang lebih murni dan representatif (Fachrunnisa, Ari Usman and Mufida Khairani, 2024). Secara keseluruhan, rangkaian preprocessing ini menciptakan dasar data visual yang bersih, seragam, dan terstruktur, yang merupakan prasyarat esensial untuk keberhasilan tahap analisis berikutnya seperti ekstraksi fitur dan klasifikasi.

2.4 Tanda Tangan Digital

Tanda tangan digital adalah sebuah konsep dalam keamanan siber dan hukum digital yang merujuk pada mekanisme kriptografi untuk memastikan keaslian, integritas, dan nirpenyangkalan (non-repudiation) dari suatu dokumen atau pesan elektronik (Mar'ah *et al.*, 2025). Berbeda dengan tanda tangan konvensional yang dihasilkan secara manual, tanda tangan digital dihasilkan secara

matematis menggunakan algoritma kriptografi kunci-asimetris. Dengan demikian, tanda tangan digital tidak hanya mengidentifikasi penanda tangan, tetapi juga menjamin bahwa dokumen tidak mengalami perubahan sedikit pun setelah ditandatangani (Indriani.S *et al.*, 2024).

Namun, penting untuk membedakannya dari tanda tangan elektronik hasil pindaian (atau digitized signature), yang sering kali menjadi fokus dalam penelitian pengolahan citra dan biometrik seperti deteksi pemalsuan. Dalam konteks tersebut, tanda tangan digital sering diartikan sebagai representasi grafis atau citra dari tanda tangan tulisan tangan yang diambil secara offline (hasil scan) atau online (direkam via tablet). Penelitian deteksi pemalsuan biasanya berfokus pada jenis yang kedua ini, dengan menganalisis karakteristik bentuk, tekanan, dan dinamika goresan untuk membedakan keaslian dari pemalsuan.



Gambar 2.2 Contoh Tanda Tangan Digital

2.5 Ekstraksi Fitur

Ekstraksi fitur adalah suatu proses fundamental dalam pengolahan citra dan pembelajaran mesin di mana karakteristik atau atribut paling informatif dan pembeda diidentifikasi serta dihitung dari data mentah (seperti citra) untuk menghasilkan representasi yang lebih ringkas dan bermakna. Tujuannya adalah

untuk mentransformasikan data berdimensional tinggi—seperti piksel dalam citra—menjadi sekumpulan nilai numerik atau deskriptor (vektor fitur) yang mampu mewakili sifat-sifat penting objek secara efektif, sekaligus mengurangi redundansi dan dimensi data (Lusiana, Al Amin and Hartono, 2024). Dalam konteks penelitian seperti deteksi pemalsuan tanda tangan, ekstraksi fitur bertindak sebagai langkah kritis yang "menangkap" pola unik dari tanda tangan asli, misalnya dengan menggunakan HU Moments yang mengekstraksi tujuh nilai invarian yang merepresentasikan bentuk global. Fitur-fitur terpilih ini kemudian menjadi input untuk belajar membedakan antara pola asli dan palsu. Dengan demikian, ekstraksi fitur berperan sebagai jembatan antara data visual mentah dan keputusan analitis, di mana keberhasilan sistem secara keseluruhan sangat bergantung pada kualitas dan relevansi fitur yang diekstraksi (Rosiva *et al.*, 2023).

2.6 Hu Moment

Metode Hu Moments pada citra digital adalah teknik ekstraksi fitur berbasis momen yang digunakan untuk mendeskripsikan karakteristik bentuk global suatu objek dalam citra, dengan sifat invarian terhadap translasi, penskalaan, dan rotasi. Dalam konteks deteksi keaslian tanda tangan, metode ini diterapkan setelah tahap pra-pemrosesan citra (seperti grayscaling, binerisasi, dan penghilangan noise) untuk mengubah bentuk tanda tangan yang unik menjadi tujuh nilai numerik yang merepresentasikan distribusi spasial pikselnya (Cahya, Pebrianto and M, 2021). Ketujuh nilai ini dihitung dari kombinasi momen pusat ternormalisasi, yang mampu menangkap esensi geometris tanda tangan seperti elongasi, kebulatan, dan asimetri—ciri-ciri yang sulit ditiru secara sempurna oleh pemalsu. Keunggulan

utama Hu Moments terletak pada kemampuannya menghasilkan deskriptor yang konsisten terlepas dari posisi, ukuran, atau orientasi tanda tangan dalam citra, sehingga sangat cocok untuk analisis tanda tangan offline yang diperoleh dari pindaian dengan variasi pengambilan gambar (Waluyo Poetro *et al.*, 2024). Namun, karena hanya fokus pada bentuk global, metode ini sering dikombinasikan dengan fitur lain (seperti tekstur atau contour-based features) untuk meningkatkan akurasi sistem dalam membedakan tanda tangan asli yang halus dan alami dari pemalsuan yang cenderung kaku atau tidak konsisten. Dengan demikian, Hu Moments berperan sebagai fitur pembeda untuk mengidentifikasi keaslian tanda tangan secara otomatis dan andal (Kurniawan, Soemarto and Yahya, 2021).

Proses deteksi keaslian tanda tangan digital menggunakan metode Hu Moments. Proses dimulai dari citra tanda tangan yang telah dipraproses, kemudian dilakukan ekstraksi fitur Hu Moments, yaitu menghitung tujuh nilai momen invarian yang merepresentasikan karakteristik bentuk tanda tangan. Nilai-nilai ini bersifat stabil terhadap perubahan rotasi, skala, dan translasi sehingga mampu menangkap pola unik dari setiap tanda tangan. Selanjutnya fitur yang diperoleh dibandingkan dengan fitur dari tanda tangan referensi melalui tahap klasifikasi atau pengukuran kemiripan untuk menentukan tingkat kesesuaian (Riskha, 2024). Berdasarkan hasil perbandingan tersebut, sistem akhirnya memberikan keputusan apakah tanda tangan termasuk asli atau palsu, sehingga metode Hu Moments efektif digunakan sebagai representasi bentuk dalam proses identifikasi keaslian tanda tangan digital.

2.7 Pengujian

Pengujian menggunakan confusion matrix dalam penelitian deteksi pemalsuan tanda tangan digital merupakan metode evaluasi kinerja model klasifikasi yang penting untuk mengukur seberapa akurat sistem dapat membedakan antara tanda tangan asli (genuine) dan tanda tangan palsu (forgery) (Humaidi and Maulani, 2023). Confusion matrix menyajikan performa model dalam bentuk matriks yang membandingkan hasil prediksi dengan label sebenarnya, menghasilkan empat kategori kunci: True Positive (TP) yang menandakan jumlah tanda tangan asli yang berhasil dikenali sebagai asli, True Negative (TN) yang menunjukkan tanda tangan palsu yang berhasil diidentifikasi sebagai palsu, False Positive (FP) yang terjadi ketika tanda tangan palsu salah diklasifikasikan sebagai asli (kesalahan tipe I atau false acceptance), dan False Negative (FN) ketika tanda tangan asli justru dikenali sebagai palsu (Elvin and Lubis, 2022).

Dalam konteks keamanan biometrik seperti verifikasi tanda tangan, kedua jenis kesalahan ini memiliki implikasi kritis: false acceptance dapat membahayakan sistem dengan mengizinkan akses palsu, sementara false rejection dapat mengganggu pengguna sah dan mengurangi kepuasan pengguna. Dari keempat nilai dasar ini, berbagai metrik performa dapat dihitung, seperti akurasi yang mengukur persentase klasifikasi benar secara keseluruhan, presisi yang menilai keandalan sistem dalam memprediksi keaslian, recall (sensitivity) yang mengukur kemampuan sistem mendeteksi semua tanda tangan asli yang ada, dan F1-score sebagai harmonisasi antara presisi dan

recall (Apridiansyah *et al.*, 2025). Confusion matrix juga memungkinkan peneliti menganalisis pola kesalahan, misalnya apakah model cenderung lebih rentan terhadap jenis pemalsuan tertentu, sehingga dapat menjadi dasar untuk penyempurnaan fitur atau algoritma klasifikasi. Dengan demikian, confusion matrix tidak hanya memberikan gambaran menyeluruh tentang efektivitas model, tetapi juga membantu dalam menyeimbangkan trade-off antara tingkat keamanan dan kenyamanan pengguna dalam pengembangan sistem deteksi pemalsuan tanda tangan digital yang andal.