ISSN: 2614-6754 (print)
ISSN: 2614-3097(online)

Halaman 27589-27597
Volume 9 Nomor 2 Tahun 2025

Penerapan Sistem Pendeteksian Pemalsuan Tanda Tangan Berbasis *Optical Character Recognition* (OCR) dan *Support Vector Machine* (SVM)

Puti Zafania[1], Hadi Kurnia Saputra[2], Dony Novaliendry[3], Syukhri[4]
[1] Informatika, Universitas Negeri Padang
[2,3,4] Teknik Elektronika, Universitas Negeri Padang
e-mail: putizafania6@gmail.com

Abstrak

Penelitian ini bertujuan mengembangkan sistem deteksi pemalsuan tanda tangan basah pada dokumen resmi dengan menggabungkan *Optical Character Recognition* (OCR) dan *Support Vector Machine* (SVM). Data terdiri atas 760 sampel tanda tangan asli dan palsu yang diperoleh dari pemindaian dokumen fisik dan pelabelan kategori. Sistem mendeteksi dan mengekstraksi area tanda tangan menggunakan OCR, lalu mengklasifikasikannya dengan SVM berbasis fitur *Histogram of Oriented Gradients* (HOG). Pengembangan dilakukan menggunakan metode *prototyping* dan diuji melalui *integration testing*. Hasil menunjukkan SVM dengan *kernel* RBF membedakan tanda tangan asli dan palsu dengan akurasi tinggi. Integrasi OCR dan SVM terbukti efektif serta efisien untuk verifikasi tanda tangan pada dokumen resmi.

Kata kunci: *Deteksi Pemalsuan Tanda Tangan, Optical Character Recognition, Support Vector Machine, Metode Prototyping, Integration Testing.*

Abstract

This study aimed to develop a forged wet signature detection system for official documents by integrating Optical Character Recognition (OCR) and Support Vector Machine (SVM). The dataset included 760 genuine and forged signatures obtained from scanned physical documents and labeled accordingly. The system detects and extracts signature areas using OCR, then classifies them with SVM based on Histogram of Oriented Gradients (HOG) features. Development used the prototyping method and was tested through integration testing. The results show that the SVM model with an RBF kernel distinguishes genuine from forged signatures with high accuracy. OCR and SVM integration proves effective and efficient for signature verification in official documents.

Keywords : *Signature Forgery Detection, Optical Character Recognition, Support Vector Machine, Prototyping Method, Integration Testing.*

PENDAHULUAN

Tanda tangan merupakan hasil proses menulis dari seseorang yang bersifat khusus sebagai substansi simbolik dan menjadi gambaran asli dari identitas pemilik yang bersifat legal (Reswan & Gunawan, 2021). Dalam kehidupan sehari-hari, tanda tangan digunakan sebagai identifikasi dari pemiliknya. Keberadaan tanda tangan dalam sebuah dokumen menyatakan bahwa pihak yang menandatangani mengetahui dan menyetujui atau mengesahkan seluruh isi dari dokumen (Husna & Novia Rizki, 2023).

Pada tahun 2025, penggunaan tanda tangan elektronik dan tanda tangan digital meningkat drastis sebanyak 754 juta dalam waktu 5 tahun(Juro, 2024). Namun pada praktiknya, tanda tangan basah masih menjadi bentuk autentikasi utama dalam berbagai dokumen resmi di Indonesia. Berdasarkan Pasal 60 ayat 2 Peraturan Pemerintah Republik Indonesia Nomor 71 Tahun 2019, dalam hal terdapat peraturan perundang-undangan yang mengatur secara khusus penggunaan tanda tangan elektronik atau mensyaratkan penggunaan tanda tangan basah, maka ketentuan umum mengenai tanda tangan elektronik tidak berlaku(Peraturan Pemerintah Republi Indonesia, 2019).

Keaslian tanda tangan sangat penting untuk memastikan validitas dokumen dan mencegah tindakan pemalsuan yang dapat merugikan individu maupun institusi. Proses validasi tanda tangan dapat dilakukan dengan pemeriksaan terhadap tanda tangan referensi dan pemeriksaan oleh ahli (Auctions, 2025). Validasi berdasarkan referensi relatif mudah dilakukan pada jumlah dokumen yang sedikit, namun menjadi lebih kompleks ketika jumlah dokumen meningkat(Octariadi, 2020).

Kasus pemalsuan tanda tangan dan dokumen di Indonesia telah banyak terjadi dan merugikan banyak pihak. Sebagai contoh, tahun 2023 terjadi kasus pemalsuan tanda tangan kadus-kades oleh oknum anggota DPRD(Said, 2025). Kasus lain terjadi di PT Citra Lampia Mandiri yang mengalami kerugian bernilai Rp4.875.000.000.000 akibat pemalsuan tanda tangan atas akta pemilik sah saham(Integra Teknologi Solusi, 2023). Hukum pidana Indonesia mengatur mengenai pemalsuan tanda tangan dalam KUHP Pasal 263 dan Pasal 264 dengan ancaman hukuman penjara maksimal 6-8 tahun.

Seiring meningkatnya penggunaan dokumen digital, teknologi pendeteksi berbasis komputer seperti Optical Character Recognition (OCR) mulai banyak dikembangkan untuk membantu proses identifikasi dan validasi dokumen yang mengandung tanda tangan. Metode OCR merupakan salah satu pendekatan yang banyak digunakan dalam proses pengenalan dan validasi tanda tangan(Rizal Toha & Triayudi, 2022). Teknologi OCR, khususnya Pytesseract OCR, telah terbukti efektif dalam mengekstraksi informasi dari dokumen dengan akurasi tinggi mencapai 90%(Nisha, 2024).

Metode Support Vector Machine (SVM) merupakan salah satu teknik yang umum digunakan dalam pengenalan pola dan klasifikasi, termasuk dalam deteksi pemalsuan tanda tangan. Algoritma ini dipilih karena memiliki kemampuan memisahkan dua kelas dengan margin maksimum, sehingga menghasilkan akurasi yang tinggi serta lebih tahan terhadap overfitting(Tariq et al., 2023). .Penelitian menunjukkan bahwa penggunaan Gabor Filter, HSV, GLCM, dan SVM dapat mencapai akurasi 99,43% pada pengenalan tanda tangan untuk validasi dokumen (Pujianto et al., 2021).

Gap penelitian terkait integrasi OCR dan SVM secara langsung untuk mendeteksi tanda tangan palsu masih jarang dibahas secara mendalam. Oleh karena itu, penelitian ini bertujuan untuk mengembangkan sistem pendeteksi pemalsuan tanda tangan basah dengan mengintegrasikan teknologi OCR untuk ekstraksi fitur dan SVM untuk klasifikasi, sehingga diharapkan dapat memberikan solusi yang lebih efektif dan efisien dalam mendeteksi pemalsuan tanda tangan.

METODE

Subjek dan Data Penelitian

Penelitian ini menggunakan data primer yang dikumpulkan melalui eksperimen dengan metode observasi langsung. Subjek penelitian terdiri dari 20 partisipan. Masing-masing partisipan membuat 19 tanda tangan asli sehingga diperoleh 380 sampel tanda tangan asli. Selanjutnya, setiap partisipan meniru tanda tangan milik partisipan lain sebanyak satu kali (tidak meniru tanda tangan sendiri), sehingga dihasilkan 380 tanda tangan palsu. Total dataset yang diperoleh adalah 760 sampel, dengan jumlah seimbang antara tanda tangan asli dan palsu.

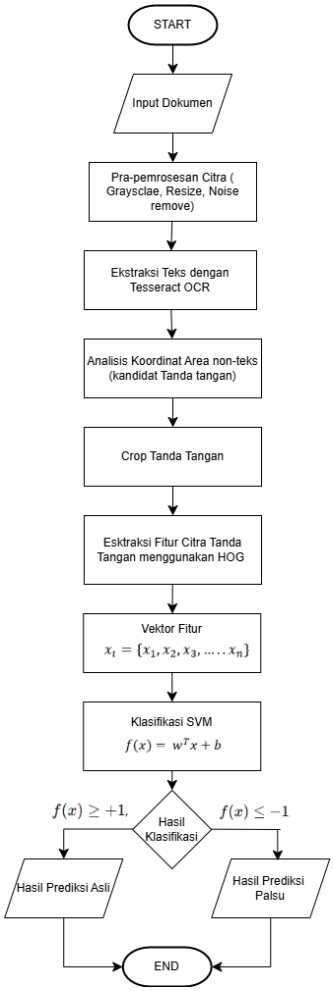
Seluruh tanda tangan dikumpulkan dalam bentuk dokumen fisik, kemudian dipindai menggunakan scanner beresolusi tinggi untuk memastikan kualitas citra optimal. Hasil pemindaian disimpan dalam format digital dan diberi label “Asli” atau “Palsu” untuk memudahkan proses pelatihan dan pengujian model.

Dataset dibagi menjadi 80% data latih dan 20% data uji. Dari total 760 sampel, sebanyak 608 digunakan sebagai data latih dan 152 sebagai data uji. Pembagian ini bertujuan menjaga keseimbangan antara jumlah data untuk pelatihan model dan jumlah data untuk evaluasi kinerja model.

Perancangan Sistem

Sistem pendeteksi pemalsuan tanda tangan dirancang untuk mengintegrasikan metode *Optical Character Recognition* (OCR) dan *Support Vector Machine* (SVM). OCR digunakan untuk mendeteksi dan mengekstraksi area tanda tangan dari dokumen, sedangkan SVM digunakan

untuk mengklasifikasikan tanda tangan menjadi kategori asli atau palsu. Proses ekstraksi fitur tanda tangan dilakukan menggunakan metode *Histogram of Oriented Gradients* (HOG).



Gambar 1. Flowchart Sistem Pendeteksian Pemalsuan Tanda Tangan

Metode Pengembangan Sistem

Metode pengembangan yang digunakan adalah prototyping. Protyping merupakan teknik pengembangan sistem yang banyak digunakan dan teknik ini juga memberikan fasilitas bagi pengembang dan pemakai untuk saling berinteraksi selama proses pembuatan, sehingga pengembang dapat dengan mudah memodelkan perangkat lunak yang akan dibuat(Kurniati, 2021).

1. **Communication**

   Sistem ini diharapkan mampu memproses dokumen yang mengandung tesk dan tanda tangan. Sistem menggunakan OCR sebagai pendeteksi Lokasi tanda tangan dan SVM untuk mengklasifikasikan tanda tangan asli dan palsu.

   Sistem yang akan dikembangkan ini menggunakan tools seperti *Pytesseract* OCR untuk preprocessing, OpenCV untuk pengolahan gambar, dan Scikit-learn untuk implementasi SVM. Bahasa pemograman yang digunakan adalah Python karena kemudahan dan kelengkapan library-nya. Framework yang digunakan yaitu Laravel untu membangun sistem pendeteksian pemalsuan tanda tangan. Framework Laravel adalah pengembangan bahasa pemograman PHP yang membantu memaksimalkan proses membantu memaksimalkan proses pengembangan wesbsite. Laravel (Alfarisi et al., 2023).

2. **Quick Plan**

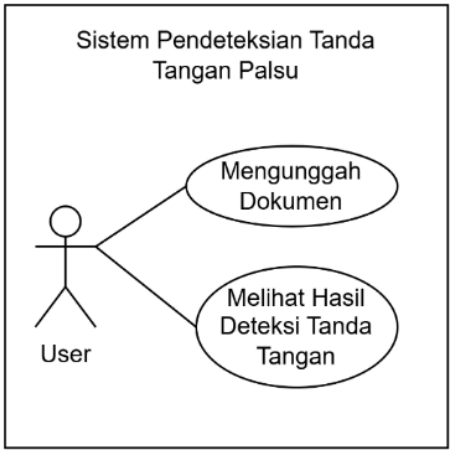
   Perencanaan penelitian diawali dengan pengumpulan dataset tanda tangan asli dan palsu, yang kemudian didigitalisasi dan diberi label sebelum digunakan pada tahap pelatihan

model. Algoritma *Support Vector Machine* (SVM) dipilih karena efektif untuk pemisahan dua kelas pada dataset berukuran kecil hingga menengah. Selain itu, dirancang antarmuka web yang menampilkan hasil deteksi beserta tingkat akurasi dalam satu halaman. Prototipe awal diuji secara internal sebelum mendapatkan umpan balik dari pengguna akhir.

3. Modelling Quick Plan

Tahap ini merupakan lanjutan dari perencanaan awal, di mana kebutuhan sistem mulai diterjemahkan ke dalam bentuk model konseptual.

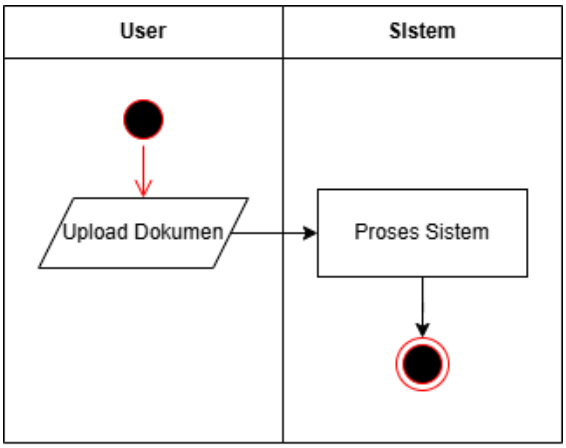
a. Use Case Diagram



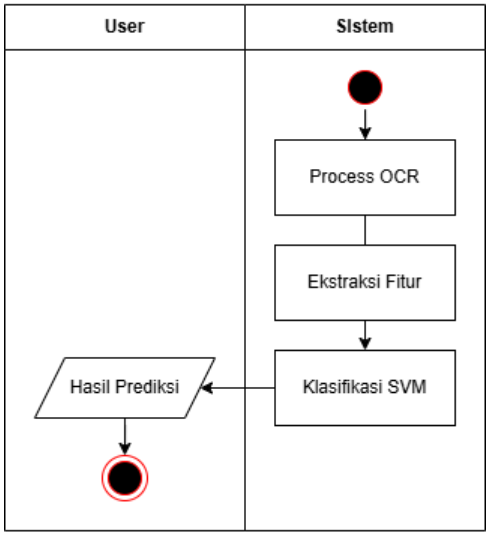
Gambar 2. Use Case Diagram Sistem

User pada sistem ini akan mengunggah dokumen yang berisikan tanda tangan yang akan dideteksi. Dokumen yang diinputkan akan dideteksi oleh sistem. Hasil deteksi akan ditampilan kepada user tanpa ada aktifitas lainnya.

b. Activity Diagram



Gambar 3. Activity Diagram Upload Dokumen Sistem



Gambar 4. Activity Diagram Hasil deteksi sistem

Activity diagram menggambarkan alur kerja sistem. Proses dimulai dengan pengguna yang mengunggah dokumen yang mengandung tanda tangan. Sistem kemudian memproses dokumen tersebut menggunakan teknologi *Optical Character Recognition* (OCR) untuk mengisolasi tanda tangan yang ada. Setelah itu, sistem mengekstrak fitur-fitur penting dari tanda tangan. Fitur-fitur yang telah diekstraksi tersebut kemudian dianalisis menggunakan algoritma *Support Vector Machine* (SVM) untuk mengklasifikasikan tanda tangan sebagai asli atau palsu. Setelah proses klasifikasi selesai, sistem akan menampilkan hasilnya kepada pengguna, dan aktivitas pun berakhir.

4. Construction Of Prototype

Perencanaan dimulai dari proses pengumpulan dataset, di mana sistem dirancang untuk membedakan antara tanda tangan asli dan palsu. Pembangunan prototipe dilakukan dengan mengimplementasikan rancangan sistem menggunakan pendekatan dua bagian utama: frontend dengan Laravel dan backend berbasis Python menggunakan Flask.

5. Deployment Delivery and Feedback

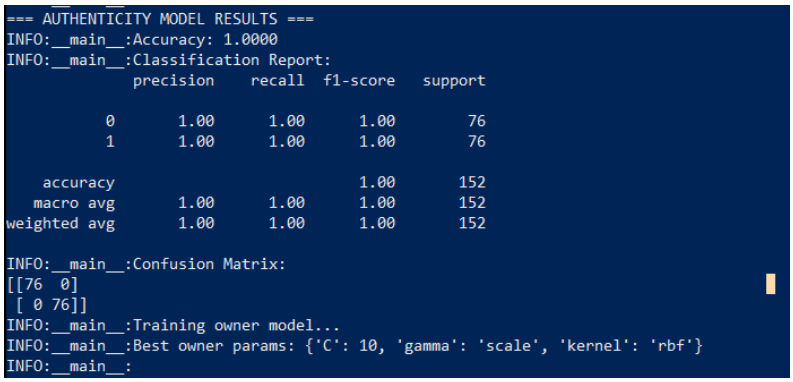
Pengujian sistem dilakukan menggunakan metode integration testing untuk memastikan keterhubungan antar modul, mulai dari input dokumen hingga klasifikasi tanda tangan dengan algoritma *Support Vector Machine* (SVM). . Keuntungan dari metode ini yaitu memberikan kepercayaan diri lebih bahwa setiap komponen yang ada dapat bekerja sama dengan baik dan mampu memberikan fungsionalitas yang diinginka (Setiawan & Risal, 2024) n. Proses diawali dengan *Pytesseract* OCR untuk mendeteksi dan mengekstraksi area tanda tangan pada dokumen, kemudian hasilnya diklasifikasikan oleh SVM sebagai asli atau palsu berdasarkan model yang telah dilatih.

Pendekatan bottom-up dan top-down testing digunakan untuk menjamin kualitas integrasi dan kestabilan sistem. Pengujian dilakukan oleh developer karena memiliki pemahaman mendalam terhadap struktur sistem, kemudian dilanjutkan uji coba oleh pengguna akhir guna memperoleh masukan terkait fungsionalitas, antarmuka, dan kemudahan penggunaan. Hasil pengujian dicatat dalam bentuk tabel dan dihitung akurasinya untuk memvalidasi kinerja sistem.

HASIL DAN PEMBAHASAN

Hasil Pengujian Model

Pengujian sistem dilakukan menggunakan dataset yang terdiri dari 760 sampel tanda tangan, terbagi seimbang antara tanda tangan asli dan palsu. Model *Support Vector Machine* (SVM) dilatih menggunakan *fitur Histogram of Oriented Gradients* (HOG) yang diekstraksi dari citra tanda tangan hasil deteksi *Optical Character Recognition* (OCR). Evaluasi kinerja model dilakukan pada data uji dengan membandingkan hasil prediksi terhadap label sebenarnya.



Gambar. 1 Hasil Model Evaluasi

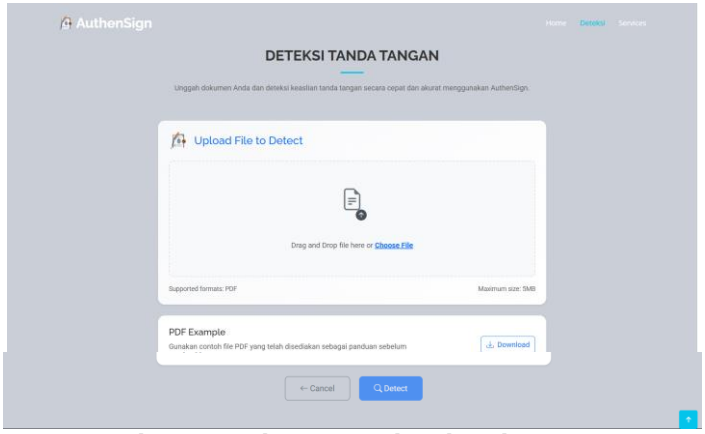
Kernel RBF memberikan margin pemisahan yang optimal antara tanda tangan asli dan palsu, sehingga menghasilkan tingkat kesalahan klasifikasi yang sangat rendah. Hal ini konsisten dengan penelitian yang menyatakan bahwa RBF efektif pada data dengan distribusi non-linear.

Pada Gambar 8, terlihat bahwa model mampu mengklasifikasikan hampir seluruh tanda tangan dengan benar pada kedua kelas. Jumlah kesalahan prediksi sangat kecil, menunjukkan keandalan sistem untuk mendeteksi tanda tangan palsu.

Implementasi Sistem

Sistem pendeteksi pemalsuan tanda tangan diimplementasikan berbasis web menggunakan framework Laravel yang terintegrasi dengan skrip Python. Pengguna cukup mengunggah dokumen, kemudian sistem secara otomatis melakukan deteksi area tanda tangan, ekstraksi fitur, dan klasifikasi hasil. Proses ini dapat dilakukan secara real-time, meminimalkan waktu verifikasi dibandingkan metode manual.

1. Halaman Upload Dokumen



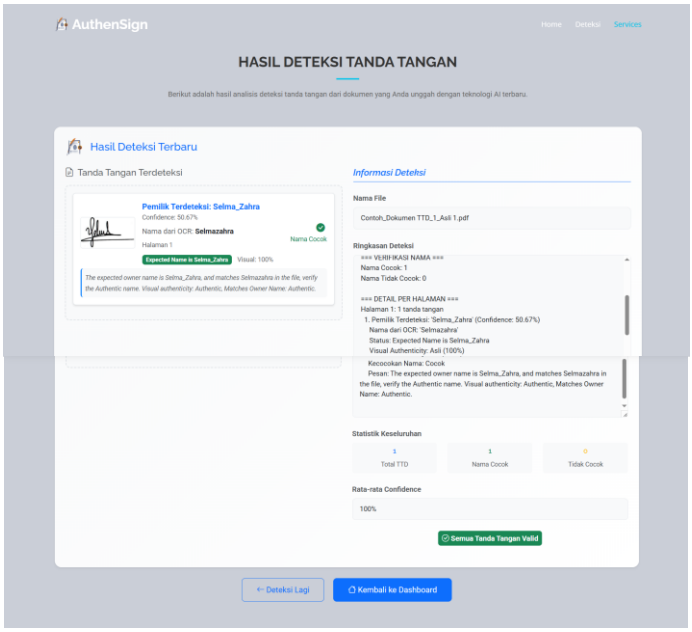
Gambar. 2 Halaman Upload Dokumen

Ketika pengguna memulai untuk mendeteksi tanda tangan, terlebih dahulu akan dialihkan pada halaman upload dokumen. Disini pengguna dapat mengupload dokumen yang ingin dideteksi yang setelah upload berhasil dapat langsung menekan tombol detect untuk menampilkan hasil analisis tanda tangan secara langsung.

2. Halaman Hasil Deteksi

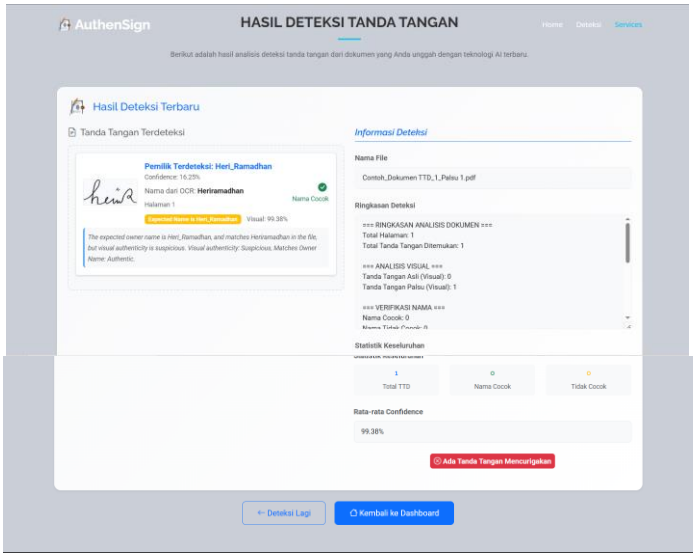
Setelah pengguna menekan tombol detect dan proses analisis dilakukan, maka akan dialihkan pada halaman ini. Dapat dilihat pada gambar dibawah ini, halaman hasil deteksi tanda tangan menampilkan tanda tangan pada dokumen yang sudah dicrop. Serta menampilkan hasil analisis dari tanda tangan tersebut. Hasil analisis menampilkan pemiliki dari

tanda tangan dan hasil akurasi dari analisis tanda tangan tersebut. Pada halaman ini akan ditampilkan apakah tanda tangan tersebut asli ataupun palsu.



Gambar. 3 Halaman Hasil Deteksi Tanda Tangan Asli

Dari gambar 10 dapat dilihat jika deteksi tanda tangan asli maka informasi yang dikeluarkan akan bewarna hijau.



Gambar. 4 Halaman Hasil Deteksi Tanda Tangan Palsu

Namun jika tanda tangan yang dideteksi Adalah palsu maka informasi yang dimunculkan akan bewarna merah.

Hasil Pengujian Sistem

Sistem akan diuji menggunakan metode integrastion testing untuk memastikan bahwa seluruh komponen dalam siste dapat berjalan dengan baik secara terpadu. Berikut hasil proses pengujian integrasi modul pada sistem yang telah dibangun:

Tabel. 1 Hasil Pengujian Sistem

No.	Skenario Pengujian	Deskripsi	Status Hasil
1.	Unggah Dokumen dengan tanda tangan asli	File pdf diuggah ke sistem, kemudian dilakukan deteksi keaslian dan kepemilikan tanda tangan	Berhasil
2.	Unggah Dokumen dengan tanda tangan palsu	Tanda tangan palsu diuggah untuk diuji keasliannya	Berhasil
3.	Unggah Dokumen dengan tanda tangan lebih dari 1 pada dokumen	File pdf yang diunggah mengandung lebih dari 1 tanda tangan untuk diuji keasliannya	Berhasil
4.	Unggah Dokumen dengan halaman lebih dari 1	Dokumen memiliki halaman yang lebih dari 1 dan tanda tangan berada halaman lain	Berhasil
5.	Tanda Tangan tidak ada dalam data pelatihan	Sistem mengklasifikasi tanda tanda tangan sebagai asing	Berhasil

Tabel 1 menujukkan hasil dari pengujian sistem ini. Dari tabel tersebut dapat diketahui bahwa seluruh komponen sistem dapat terintegrasi dengan baik. Mulai dari proses unggah dokumen, deteksi tanda tangan, esktraksi fitur, klasidifikasi, dan pengenalan pemilik dapat berjalan dengan baik.

SIMPULAN

Penelitian ini berhasil mengembangkan sistem deteksi pemalsuan tanda tangan dengan mengintegrasikan Optical Character Recognition (OCR) dan Support Vector Machine (SVM). Model klasifikasi SVM yang dibangun menunjukkan kemampuan yang sangat baik dalam membedakan tanda tangan asli dan palsu pada dataset yang digunakan, dengan tingkat akurasi tinggi. Integrasi OCR memungkinkan sistem mengekstraksi teks sekaligus mendeteksi dan memotong area tanda tangan dari dokumen secara otomatis, yang kemudian diklasifikasikan oleh SVM. Hasil pengujian melalui metode integration testing membuktikan bahwa seluruh modul sistem berfungsi secara konsisten dan mampu menangani dokumen dengan banyak tanda tangan maupun halaman, serta menampilkan hasil deteksi secara real-time. Dengan demikian, sistem ini dapat menjadi solusi efektif dan efisien dalam proses verifikasi dokumen resmi

DAFTAR PUSTAKA

Alfarisi, I. A., Priandika, A. T., & Puspaningrum, A. S. (2023). Penerapan Framework Laravel Pada Sistem Pelayanan Kesehatan (Studi Kasus: Klinik Berkah Medical Center). *Jurnal Ilmiah Computer Science*, *2*(1), 1–9. https://doi.org/10.58602/jics.v2i1.11

Auctions, B. (2025, January 25). *Autograph Authentication Guide: How to Spot Real Signatures*. Britannic Auctions.

Husna, L., & Novia Rizki, S. (2023). *Pemanfaatan JST Pengenalan Keaslian Pola Tanda Tangan untuk Pencegahan Tindakan Pemalsuan Tanda Tangan*.

Integra Teknologi Solusi. (2023, April 10). *Dugaan Pemalsuan Tanda Tangan pada PT Citra Lampia Mandiri*. Integra Teknologi Solusi. https://integrasolusi.com/inoffice/sipermen/dugaan-pemalsuan-tanda-tangan-pada-pt-citra-lampia-mandiri/

Juro. (2024, August 13). *What is a wet signature? Use cases and alternatives*. Juro. https://juro.com/learn/wet-ink-signature#

Kurniati. (2021). Penerapan Metode Prototype Pada Perancangan Sistem Pengarsipan Dokumen Kantor Kecamatan Lais. In *Journal of Software Engineering Ampera* (Vol. 2, Issue 1). https://journal-computing.org/index.php/journal-sea/index

Nisha, K. (2024). Pemeriksaan KTP Menggunakan Optical Character Recognition (OCR) Dan Pengenalan Background Serta Komponen KTP. *Universitas Muhammadiyah Makasaar*.

Octariadi, B. C. (2020). Pengenalan Pola Tanda Tangan Menggunakan Metode Jaringan Syaraf Tiruan Backpropagation. *Jurnal Teknoinfo*, *14*(1), 15. https://doi.org/10.33365/jti.v14i1.462

Peraturan Pemerintah Republi Indonesia, Pub. L. No. 71 (2019).

Pujianto, R., Lestari, M., Wayan, N., Septiani, P., Raya, J., No, T., Gedong, K., Rebo, P., & Timur, J. (2021). Pengolahan Citra Dan Metode Support Vector Machine (SVM) Dalam Pengenalan Pola Tanda Tangan. *Jurnal Rekayasa Komputasi Terapan)*, *01*, 2776–5873.

Reswan, Y., & Gunawan. (2021). Desain Aplikasi Pengenalan Pola Tanda Tangan Menggunakan Metode Support Vector Machine (SVM). In *Jurnal Media Infotama* (Vol. 17, Issue 1).

Rizal Toha, M., & Triayudi, A. (2022). Penerapan Membaca Tulisan di dalam Gambar Menggunakan Metode OCR Berbasis Website pada e-KTP. *Jurnal Sains Dan Teknologi*, *11*, 175–183. https://doi.org/10.23887/jst-undiksha.v11i1

Said, N. (2025, February 3). *Awal Mula Kasus Oknum Anggota DPRD Selayar Palsukan Tanda Tangan Kadus-Kades* **Baca artikel detiksulsel, *"Awal Mula Kasus Oknum Anggota DPRD Selayar Palsukan Tanda Tangan Kadus-Kades"*** . Detik.Com. https://www.detik.com/sulsel/hukum-dan-kriminal/d-7760547/awal-mula-kasus-oknum-anggota-dprd-selayar-palsukan-tanda-tangan-kadus-kades

Setiawan, R., & Risal. (2024). Pengembangan Unit Testing dan Integration Testing REST API Pengelola Data Bootcamp PT Mitra Integrasi Informatika. *Jurnal Strategi*, *6*.

Tariq, U., Hu, Z., Tariq, R., Iqbal, M. S., & Sadiq, M. (2023). High-Performance Embedded System for Offline Signature Verification Problem Using Machine Learning. *Electronics (Switzerland)*, *12*(5). https://doi.org/10.3390/electronics12051243