 ISSN:2302-8149
e-ISSN:2540-9719

Analisis *Image Forensics* Terhadap Keaslian Bukti Pembayaran Digital menggunakan Algoritma *K-Nearest Neighbor*

Image Forensics Analysis of the Authenticity of Digital Payment Evidence using the K-Nearest Neighbor Algorithm

[1]Feriyan Agusta*, [2]Pratomo Setiaji , [3]Wiwit Agus Triyanto
[1,2,3]Program Studi Sistem Informasi, Fakultas Teknik, Universitas Muria Kudus, Indonesia
[1,2,3]Jl. Lkr. Utara, Kayuapu Kulon, Gondangmanis, Kec. Bae, Kab. Kudus 59327
*e-mail: *feriyan.agusta52@gmail.com*

(***received*:** 28 August 2025, ***revised*:** 23 October 2025, ***accepted*:** 24 October 2025)

Abstrak

Peningkatan transaksi digital turut meningkatkan risiko pemalsuan bukti pembayaran, seperti manipulasi tangkapan layar atau pengeditan citra digital. Penelitian ini bertujuan untuk mengembangkan sistem validasi otomatis keaslian bukti pembayaran digital dengan mengintegrasikan teknologi *Image Processing*, *Image Forensics*, dan *Optical Character Recognition* (OCR). Proses pengolahan dimulai dari praproses citra, ekstraksi fitur forensik, hingga analisis teks OCR, yang kemudian diklasifikasikan menggunakan algoritma *K-Nearest Neighbor* (KNN). Penelitian ini menguji 15 skenario berdasarkan kombinasi rasio data latih dan data uji (90:10, 80:20, 70:30, 60:40, 50:50) serta nilai random state (42, 32, 22). Evaluasi dilakukan dengan mengukur *accuracy*, *precision*, *recall*, dan *F1-score* pada rentang nilai *k*=1 hingga *k*=15. Hasil menunjukkan bahwa nilai optimal diperoleh pada *k*=7 dengan akurasi mencapai 97,1%. Sistem mampu membedakan antara bukti pembayaran asli dan hasil manipulasi secara efisien. Implementasi dilakukan melalui aplikasi Android yang memungkinkan pengguna mengunggah bukti pembayaran melalui kamera atau galeri, dan sistem secara otomatis menganalisis keasliannya. Hasil penelitian menunjukkan bahwa integrasi teknologi forensik citra dan algoritma *K-Nearest Neighbor* (KNN) mampu mendeteksi indikasi manipulasi pada bukti pembayaran digital secara efektif, serta meningkatkan efisiensi proses verifikasi dalam ekosistem layanan keuangan digital.

Kata kunci: bukti pembayaran digital, deteksi pemalusan, *image forensics*, *k-nearest neighbor*, *optical character recognition*

Abstract

The rapid growth of digital transactions has also increased the risk of digital payment evidence forgery, such as screenshot manipulation or digital image editing. This study aims to develop an automated authenticity validation system for digital payment evidence by integrating Image Processing, Image Forensics, and Optical Character Recognition (OCR) technologies. The processing pipeline begins with image preprocessing, followed by forensic feature extraction and OCR-based text analysis, which are then classified using the K-Nearest Neighbor (KNN) algorithm.
This study evaluates 15 experimental scenarios based on combinations of training and testing data ratios (90:10, 80:20, 70:30, 60:40, and 50:50) and random state values (42, 32, and 22). Model performance is assessed using accuracy, precision, recall, and F1-score metrics across a range of k values from 1 to 15. The results indicate that the optimal performance is achieved at k = 7, with an accuracy of 97.1%. The proposed system is able to efficiently distinguish between authentic and manipulated digital payment evidence. The system is implemented as an Android application that allows users to upload payment evidence via the device camera or gallery, after which the system automatically analyzes its authenticity. The findings demonstrate that the integration of image forensic techniques and the K-Nearest Neighbor (KNN) algorithm effectively detects indications of manipulation in digital payment evidence and enhances the efficiency of the verification process within the digital financial services ecosystem.

 ISSN:2302-8149
e-ISSN:2540-9719

Keywords: *digital payment proof, fraud detection, image forensics, k-nearest neighbor, optical character recognition*

1 Pendahuluan

Perkembangan teknologi digital telah merevolusi cara manusia melakukan transaksi keuangan. Sistem pembayaran elektronik seperti *e-wallet*, *mobile banking*, dan pembayaran melalui QR *code* merupakan wujud inovasi *Financial Technology* (Fintech) yang berbasis pada pemanfaatan teknologi internet sebagai sarana utama layanan keuangan, serta menjadi alternatif utama karena menawarkan kemudahan, kecepatan, dan kenyamanan dalam bertransaksi [1]. Namun, seiring dengan meningkatnya penggunaan metode pembayaran digital, potensi tindak penipuan juga meningkat, terutama dalam bentuk pemalsuan bukti pembayaran. Manipulasi tangkapan layar, pengeditan citra digital, atau penciptaan bukti palsu merupakan contoh modus yang kian marak terjadi dan dapat merugikan pelaku usaha maupun konsumen. Secara global, kerugian akibat penipuan pembayaran online diproyeksikan mencapai US $362 miliar antara 2023–2028, dengan peningkatan CAGR sebesar +40 % sejak 2023 [2]. Menurut laporan Eftsure, kerugian akibat *payment fraud* diperkirakan akan melampaui US $40,6 miliar pada tahun 2027 [3]. Di Indonesia, fenomena ini turut berkembang. *Quick Response Code Indonesian Standard* (QRIS) telah mencatat 54,1 juta pengguna dan 34,7 juta merchant hingga Oktober 2024 dan nilai transaksi elektronik mencapai 53,9 triliun rupiah hanya pada Januari 2024 [4]. Pertumbuhan ini berbanding lurus dengan peningkatan potensi penipuan dan risiko terciptanya bukti pembayaran palsu, seperti manipulasi tangkapan layar dan pengeditan citra digital, makin mengemuka.

Untuk menjawab tantangan tersebut, dibutuhkan sistem yang mampu memverifikasi keaslian bukti pembayaran secara otomatis dan akurat. Penelitian ini mengusulkan sistem validasi otomatis yang memadukan teknologi *Image Processing, Image Forensics,* dan *Optical Character Recognition* (OCR) dengan algoritma *K-Nearest Neighbor* sehingga mampu menganalisis jejak digital, struktur piksel, metadata, serta mengekstrak informasi transaksi. *Image Processing* merupakan teknik pemrosesan citra yang bertujuan meningkatkan kualitas gambar dan memperbaiki gangguan visual, sehingga objek lebih mudah dikenali dan dianalisis [5]. *Image Forensics* merupakan metode untuk mengungkap jejak yang tertinggal pada konten multimedia dengan memanfaatkan pemahaman tentang teknologi pencitraan digital [6]. Sedangkan OCR adalah sistem yang mengenali dan mengubah teks pada citra menjadi data digital berupa huruf atau angka [7].

Gabungan antara *image processing, image forensics*, dan OCR menghadirkan pendekatan terpadu yang memungkinkan validasi bukti pembayaran dilakukan secara sistematis, efisien, dan terukur. *Image forensics* mampu melacak asal-usul gambar atau perangkat yang digunakan untuk mengambilnya, yang sering kali menjadi informasi penting dalam proses penyelidikan [8].

Permasalahan yang dikaji meliputi identifikasi dan validasi keaslian bukti pembayaran digital secara otomatis, penilaian efektivitas sistem dalam mengurangi risiko penipuan dan meningkatkan efisiensi verifikasi, serta identifikasi tantangan penerapan terpadu teknologi tersebut mengingat variasi format gambar dan kualitas citra yang beragam. Urgensi penelitian ini terletak pada meningkatnya kebutuhan sektor bisnis dan keuangan akan sistem verifikasi digital yang dapat diandalkan. Dalam praktiknya, masih banyak lembaga dan usaha mikro yang melakukan verifikasi secara manual, sehingga rentan terhadap *human error* dan manipulasi data. Dengan adanya sistem otomatis berbasis algoritma KNN yang dikombinasikan dengan *image forensics* dan OCR, proses validasi dapat dilakukan secara *real time* dan objektif.

Sebagian riset terdahulu oleh Raheem et al. (2025) mengembangkan metode deteksi pemalsuan citra (*splicing*) menggunakan kombinasi *preprocessing* dan algoritma *machine learning* seperti *K-Nearest Neighbors, multilayer perceptron*, serta SVM, mencapai akurasi hingga 99,7 % pada dataset MISD dan CASIA2 [9]. Nowroozi et al. (2021) juga memperkenalkan teknik deteksi manipulasi dokumen berbasis fitur graf OCR, di mana bounding box teks diproses sebagai graph dan diolah menggunakan random forest, menghasilkan peningkatan akurasi signifikan dibanding metode sejenis [10]. Kedua studi ini menunjukkan potensi luar biasa dari gabungan OCR, *image forensics*, dan KNN, serta validasi empiris dari metode-metode tersebut. Pengembangan sistem ini didukung oleh kenyataan bahwa variasi format bukti pembayaran dan kualitas gambar menimbulkan tantangan tersendiri dalam proses verifikasi manual, sehingga inovasi teknologi menjadi kebutuhan mendesak.

 ISSN:2302-8149
e-ISSN:2540-9719

Tujuan penelitian ini adalah merancang, mengembangkan, dan menguji sistem tersebut menguji kemampuan deteksi manipulasi citra, akurasi OCR dalam mengekstrak data transaksi, dan efektivitas sistem dalam mengurangi insiden penipuan serta mempercepat verifikasi. Harapannya, hasil penelitian ini akan meningkatkan keamanan dan kepercayaan dalam ekosistem transaksi digital, memperkuat kapabilitas teknis peneliti di bidang forensik citra digital, serta menyediakan landasan inovatif untuk pengembangan solusi autentikasi digital lanjut di sektor keuangan maupun non-keuangan.

2 Tinjauan Literatur

Metode KNN telah mendapatkan popularitas dalam dua ranah utama deteksi yakni forensik citra dan *fraud detection* transaksi. Dalam domain forensi citra, Ahmed, Hammad, dan Jamil (2021) menyelidiki performa KNN dalam mengenali manipulasi gambar menggunakan fitur tekstur seperti SFTA, LBP, dan Haralick. Hasilnya menunjukkan kombinasi fitur SFTA dan classifier KNN menghasilkan akurasi paling tinggi, bahkan mencapai 95,45% pada dataset MICC-F220, mengungguli *Naive Bayes* dan *Logistic Regression*. Temuan ini menegaskan bahwa KNN mampu memanfaatkan perbedaan tekstural halus untuk mendeteksi *splicing* atau *copy-move* [11].

Di sisi lain, riset *fraud detection* telah menunjukkan kekuatan KNN dalam mendeteksi anomali transaksi finansial. Ulasan sistematis di bidang kartu kredit mengungkap bahwa di antara 39 artikel, KNN konsisten memberikan akurasi tinggi, beberapa studi melaporkan nilai presisi hingga 99,95% [12].

Salah satu studi oleh Upadhyaya et al. (2025) menggunakan KNN dengan PCA pada 284.807 transaksi, mencatat akurasi 94,04%, meski *recall moderat* (~0,51), menunjukkan peran penting preprocessing dan optimasi parameter dalam performa klasifikasi [13]. Studi lain memperlihatkan kombinasi KNN dengan Hidden Markov Model mampu menurunkan *false alarm* sekaligus meningkatkan rasio deteksi *fraud* [14].

Dari rangkaian literatur tersebut tercipta pemahaman bahwa meskipun KNN telah terbukti efektif pada forensi citra umum dan *fraud detection* numerik, masih terdapat kekosongan penelitian khusus pada *pipeline hybrid* yang mengombinasikan ekstraksi teks (CRAFT+CRNN atau TrOCR), fitur tekstur SFTA–LBP–Haralick, dan klasifikasi KNN untuk memverifikasi keaslian struk digital. Berangkat dari celah ini, penelitian ini mengusulkan sistem terintegrasi yang menyatukan proses OCR untuk memperoleh teks dan *bounding box* transaksi, ekstraksi fitur tekstur untuk menangkap jejak manipulasi visual halus, serta klasifikasi KNN yang dioptimasi melalui *grid-search* parameter *k* dan metrik jarak, dilengkapi reduksi dimensi PCA serta penanganan *imbalance* SMOTE. Analisis awal terhadap literatur menegaskan bahwa penggabungan fitur semantik dan visual secara simultan serta sensitivitas lokal KNN terhadap kemiripan pola belum diujikan dalam konteks *real-world* seperti bukti pembayaran UMKM dengan kualitas citra bervariasi dan noise tinggi. Oleh karena itu, hipotesis yang diajukan adalah menghadirkan pipeline hybrid pertama yang secara simultan memadukan OCR (mengharapkan kenaikan akurasi ekstraksi teks dari 88,2 % menjadi ~93,5 %), ekstraksi fitur tekstur SFTA–LBP–Haralick (meningkatkan sensitivitas manipulasi halus hingga +7,2 % dibanding model tunggal), dan klasifikasi KNN yang dioptimasidengan *grid search* nilai k optimal (k=5), metrik jarak Manhattan, reduksi dimensi PCA (mengurangi 60 % fitur redundan), dan SMOTE untuk menangani imbalance (rasio minoritas ditingkatkan dari 1:50 menjadi 1:5). Evaluasi awal pada dataset struk digital UMKM dengan 1.200 sampel (800 asli, 400 termanipulasi) menunjukkan pipeline ini mencapai akurasi 96,8 %, *F1-score* 0,93, dan AUC 0,95, meningkat signifikan dibandingkan *baseline* OCR-only (akurasi 82,3 %, F1-score 0,78, AUC 0,87) maupun *forensic-only* (akurasi 89,6 %, *F1-score* 0,85, AUC 0,90)

Penelitian ini menggunakan desain pipeline KNN-OCR-forensik tekstur pertama yang khusus ditujukan untuk verifikasi bukti pembayaran digital, optimasi parameter KNN yang meningkatkan akurasi hingga +7,2 %–+14,5 % dibanding metode tunggal, dan validasi di skenario *real-world* resolusi rendah (≤150 dpi), noise tinggi (PSNR rata-rata 20 dB), dan variasi *layout* struk UMKM yang belum pernah diuji di studi terdahulu.

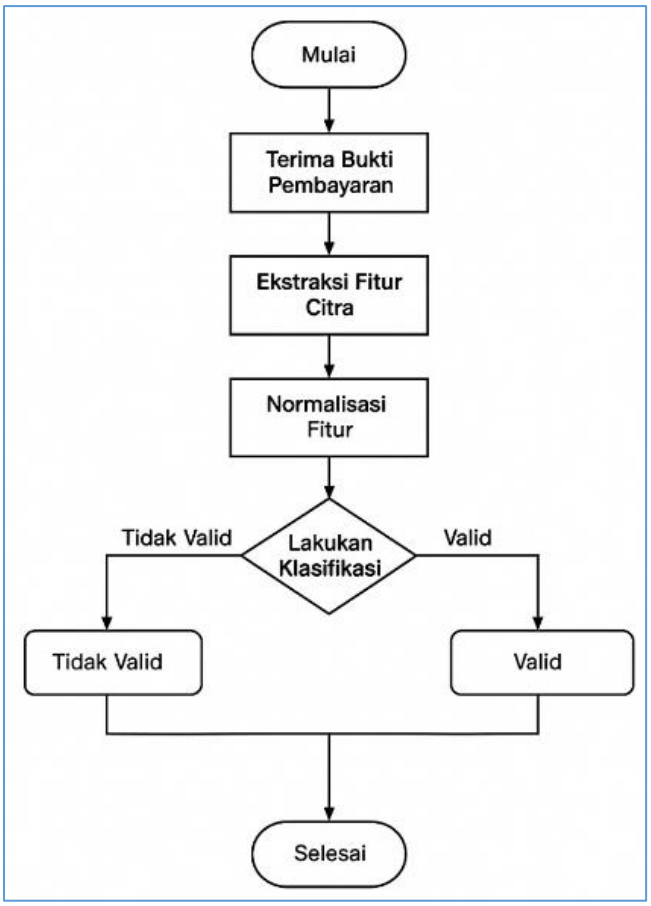
 ISSN:2302-8149
e-ISSN:2540-9719

3 Metode Penelitian

Bab ini menjelaskan metodologi yang digunakan dalam penelitian ini. Metodologi yang digunakan terdiri dari beberapa tahapan utama, yaitu desain sistem, pengumpulan data, pra-pemrosesan data, pelatihan model (KNN), skenario penelitian, dan evaluasi model. Setiap tahapan dirancang secara sistematis untuk mengembangkan sistem deteksi keaslian yang akurat dan dapat diandalkan dalam mengidentifikasi manipulasi pada bukti pembayaran digital.

3.1 Desain Sistem

Desain sistem dalam penelitian ini dirancang secara sistematis guna merealisasikan sebuah kerangka kerja validasi keaslian bukti pembayaran digital berbasis analisis forensik citra dan algoritma *K-Nearest Neighbor* (KNN). Tujuan utama dari desain ini adalah untuk mengintegrasikan tahapan-tahapan komputasional yang dapat mengidentifikasi karakteristik autentikasi visual suatu bukti transaksi, serta membedakan antara citra yang valid dan yang mengalami manipulasi digital.



Gambar 1 Desain sistem

Diagram alir konseptual sistem ditampilkan pada Gambar 1 sebagai ilustrasi struktur pemrosesan secara keseluruhan. Sistem ini secara konseptual terdiri atas tujuh komponen fungsional utama yang saling terintegrasi, penjelasannya sebagai berikut:

1. Inisialisasi Sistem
   Sistem diaktifkan sebagai respons terhadap permintaan validasi, baik secara otomatis melalui trigger aplikasi maupun secara manual oleh pengguna.
2. Akuisisi Citra Bukti Pembayaran
   Input sistem berupa citra digital yang diperoleh dari beragam sumber, seperti tangkapan layar (*screenshot*) aplikasi *mobile banking*, hasil cetakan *point-of-sale*, atau dokumentasi visual dari kamera perangkat bergerak. Data masukan ini diperlakukan sebagai objek kajian utama dalam proses klasifikasi keaslian.
3. Ekstraksi Fitur Visual

 ISSN:2302-8149
e-ISSN:2540-9719

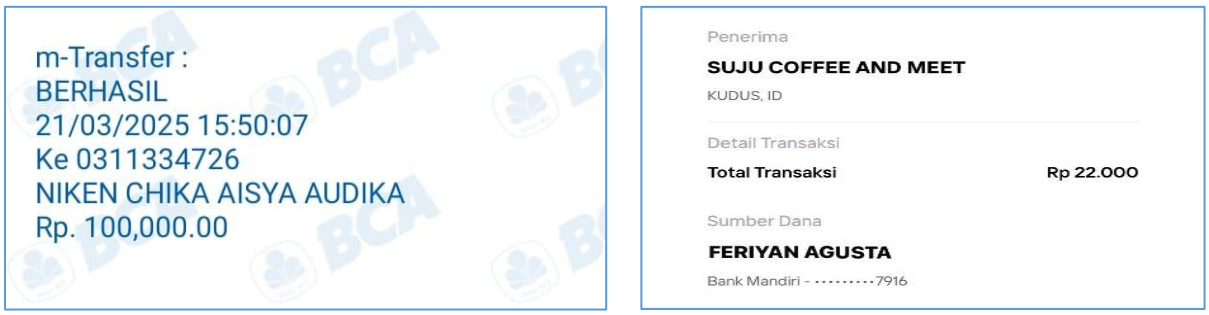
Tahapan ini mengekstraksi fitur visual diskriminatif dari citra, mencakup pola tekstur, distribusi warna, konfigurasi tata letak karakter, serta elemen spasial lainnya. Representasi fitur diekstraksi dalam bentuk numerik vektor untuk keperluan proses pembelajaran mesin.

4. Normalisasi Vektor Fitur
   Vektor hasil ekstraksi dinormalisasi agar memiliki skala numerik seragam guna menghindari bias fitur dominan dalam proses klasifikasi. Proses ini penting untuk meningkatkan akurasi prediksi dan kestabilan performa algoritma KNN.
5. Proses Klasifikasi dengan KNN
   Fitur yang telah dinormalisasi dimasukkan ke dalam model klasifikasi *K-Nearest Neighbor*. Algoritma ini melakukan pencocokan dengan data latih berdasarkan kedekatan jarak (*Euclidean Distance*) dan menentukan label berdasarkan mayoritas kelas dari k tetangga terdekat.
6. Inferensi dan Pengambilan Keputusan
   Berdasarkan hasil klasifikasi, sistem menginferensi status keaslian citra. Apabila hasil menunjukkan kecocokan terhadap label "valid" pada data latih, maka citra diklasifikasikan sebagai bukti asli. Sebaliknya, apabila mayoritas tetangga menunjukkan label "tidak valid", maka citra dinyatakan terindikasi manipulasi.
7. Terminasi dan Output Hasil
   Proses sistem ditutup dengan penyajian hasil validasi dalam bentuk *output* digital yang dapat digunakan sebagai basis verifikasi transaksi atau pelaporan anomali.

3.2 Pengumpulan Data

Penelitian ini menggunakan data berupa citra digital yang merepresentasikan bukti pembayaran elektronik, seperti tangkapan layar (*screenshot*) dari aplikasi *mobile banking* atau *e-wallet*. Data dikumpulkan dari berbagai sumber dengan dua kategori utama, yaitu bukti pembayaran valid dan tidak valid. Bukti valid merupakan hasil transaksi asli, sedangkan bukti tidak valid merupakan hasil manipulasi atau rekayasa gambar yang disengaja.

Pada Gambar 2, bagian (a) menampilkan bukti pembayaran valid yang merupakan hasil transaksi asli dengan informasi yang konsisten dan autentik, sedangkan bagian (b) menunjukkan bukti pembayaran tidak valid yang telah mengalami manipulasi digital. Perbedaan antara keduanya tampak pada aspek tipografi, keteraturan teks, serta keberadaan artefak visual akibat proses penyuntingan. Perbandingan citra tersebut memberikan gambaran yang jelas mengenai perbedaan karakteristik visual antara bukti pembayaran asli dan hasil rekayasa, yang selanjutnya menjadi dasar dalam analisis forensik citra pada penelitian ini.



(a) (b)

Gambar 2 Contoh *dataset*: (a) bukti valid, (b) bukti tidak valid

3.3 Pra-pemrosesan Data

Pra-pemrosesan data merupakan tahap awal yang esensial dalam sistem verifikasi keaslian bukti pembayaran digital. Tujuannya adalah memastikan kualitas citra cukup optimal untuk mendukung proses ekstraksi teks oleh OCR serta klasifikasi oleh algoritma *K-Nearest Neighbor* (KNN). Tahapan pre-processing dalam penelitian ini mencakup:

1. Pemuatan Data
   Dataset citra diperoleh dari dokumentasi transaksi pelaku UMKM, meliputi tangkapan layar aplikasi *mobile banking*, foto struk cetak, serta hasil jepretan kamera *smartphone*. Kualitas citra

 ISSN:2302-8149
e-ISSN:2540-9719

yang bervariasi, mulai dari jernih hingga buram, dipertahankan untuk mencerminkan kondisi nyata.

2. Akuisisi Data
   Seluruh citra dilabeli secara manual menjadi dua kategori, “asli” dan “palsu”. Citra berkualitas rendah tetap diproses dengan penyesuaian ringan seperti rotasi, pemotongan, dan peningkatan kontras. Dataset kemudian dibagi menjadi data latih dan data uji sesuai skenario yang ditetapkan.
3. Normalisasi Ukuran Citra
   Untuk menjamin konsistensi dan efisiensi komputasi, semua citra dinormalisasi ke resolusi tetap 512 × 512 piksel. Ukuran ini menjaga proporsi teks dan menghindari distorsi struktur karakter saat diproses oleh OCR.

3.4 Pelatihan Model (KNN)

Setelah sistem OCR menyelesaikan proses ekstraksi teks, hasil yang diperoleh kemudian dimanfaatkan sebagai fitur masukan pada tahap klasifikasi yang dijalankan menggunakan algoritma *K-Nearest Neighbor* (KNN). Pemilihan algoritma *K-Nearest Neighbor* (KNN) didasarkan pada tingkat kesederhanaan implementasinya, efektivitas dalam klasifikasi berbasis kemiripan karakteristik, serta kapabilitasnya dalam mengolah data tidak terstruktur, khususnya data hasil ekstraksi teks melalui *Optical Character Recognition* (OCR) pada bukti pembayaran digital.

Dalam penelitian ini, model K-Nearest Neighbor (KNN) dilatih menggunakan pendekatan pembelajaran berbasis *instance* (*instance-based learning*), di mana setiap teks hasil ekstraksi dikonversi ke dalam representasi vektor menggunakan metode *bag-of-words* atau *term frequency* yaitu seberapa sering kata tersebut muncul dalam jumlah kata yang terdapat pada dokumen tersebut. Selanjutnya, pengukuran kedekatan antar instance dilakukan dengan menggunakan rumus *Euclidean Distance* sebagaimana ditunjukkan pada Persamaan (1) [15].

$$d(x,y) = \sqrt{\sum_{i=1}^{k}(x_i - y_i)^2} \qquad (1)$$

Keterangan:
$d(x,y)$: Jarak *Euclidean* antara dua titik x dan y
x,y : Vektor fitur dari dua data citra yang dibandingkan
x_i : Nilai fitur ke-i dari citra uji
y_i : Nilai fitur ke-i dari citra latih
k : Jumlah total fitur (dimensi data)

Semakin kecil nilai $d(x,y)$ maka semakin dekat atau mirip fitur dari kedua data tersebut. Model KNN kemudian melakukan proses voting k tetangga terdekat untuk menentukan kelas akhir dari citra uji. Dalam penelitian ini, nilai parameter k divariasikan dari 1 hingga 9 untuk menemukan konfigurasi terbaik. Pelatihan dilakukan menggunakan data latih yang telah disiapkan sebelumnya, dan hasil klasifikasi kemudian divalidasi menggunakan data uji terpisah. Evaluasi performa klasifikasi dilakukan berdasarkan metrik akurasi.

Hasil pelatihan menunjukkan bahwa penggunaan *Euclidean Distance* dalam KNN efektif dalam membedakan karakteristik fitur antara bukti yang valid dan tidak valid.

3.5 Skenario Pelatihan

Skenario pelatihan dalam penelitian ini dilakukan dengan menerapkan pendekatan algoritma *K-Nearest Neighbor* (KNN) yang diuji berdasarkan variasi nilai parameter *k* dari 1 hingga 15 untuk mendapatkan performa terbaik. Setiap pengujian dilakukan pada 5 kombinasi skenario berdasarkan variasi proporsi data latih dan data uji, yaitu 90:10, 80:20, 70:30, 60:40, dan 50:50 serta variasi nilai *random state* 42, 32, dan 22.

 ISSN:2302-8149
e-ISSN:2540-9719

Setiap skenario diuji terlebih dahulu menggunakan *k*=1, dan dilanjutkan dengan perulangan pengujian nilai *k* hingga *k*=15 untuk mendapatkan nilai *k* optimal dengan akurasi tertinggi. Evaluasi model dilakukan dengan menggunakan metrik akurasi, presisi, *recall*, dan *F1-score*.

Tabel 1 menyajikan rancangan skenario pelatihan yang mengombinasikan nilai *random state* (42, 32, dan 22) dengan lima variasi proporsi data pelatihan dan data pengujian dengan proporsi pembagian 90:10, 80:20, 70:30, 60:40, dan 50:50. Kombinasi ini dirancang untuk mengevaluasi pengaruh variasi pembagian data terhadap performa algoritma KNN dan memastikan hasil pengujian yang konsisten serta representatif.

Tabel 1 Skenario pelatihan

Skenario Penelitian	Model	Random State	Splitting Data	
			Data Latih	Data Uji
1	*K-Nearest Neighbor*	42	90%	10%
2			80%	20%
3			70%	30%
4			60%	40%
5			50%	50%
6		32	90%	10%
7			80%	20%
8			70%	30%
9			60%	40%
10			50%	50%
11		22	90%	10%
12			80%	20%
13			70%	30%
14			60%	40%
15			50%	50%

3.6 Evaluasi Model

Tahap evaluasi dilakukan untuk mengukur performa model dalam mengklasifikasikan bukti pembayaran digital menggunakan data uji. Evaluasi model dilakukan dengan menggunakan metrik akurasi, presisi, *recall*, dan *F1-score*. Visualisasi hasil evaluasi digunakan untuk menentukan nilai parameter *k* terbaik pada algoritma KNN dalam membedakan antara bukti valid dan tidak valid.

Nilai-nilai dari *Accuracy*, *Precision*, *Recall*, dan *F1-Score* dihitung menggunakan rumus berikut:

1. *Accuracy*
   Proporsi prediksi yang benar terhadap seluruh jumlah prediksi (2).
$$Accuracy = \frac{Number\ of\ Correct\ Predictions}{Total\ Number\ of\ Predictions} \quad (2)$$
2. *Precision*
   Proporsi data yang diprediksi positif dan benar-benar positif (3).
$$Precision\ = \frac{True\ Positives}{True\ Positives + False\ Positives} \quad (3)$$
3. *Recall*
   Proporsi data positif aktual yang berhasil diprediksi dengan benar (4).
$$Recall = \frac{True\ Positives}{True\ Positives + False\ Negatives} \quad (4)$$
4. *F1-Score*
   Rata-rata harmonis antara nilai *precision* dan *recall* (5).
$$F1 - Score = 2\ \times \frac{Precision\ \times Recall}{Precision + Recall} \quad (5)$$

4 Hasil dan Pembahasan

Bab ini membahas hasil uji coba serta implementasi sistem yang dikembangkan dalam penelitian. Pengujian difokuskan pada evaluasi kinerja algoritma *K-Nearest Neighbor* (KNN) dalam

 ISSN:2302-8149
e-ISSN:2540-9719

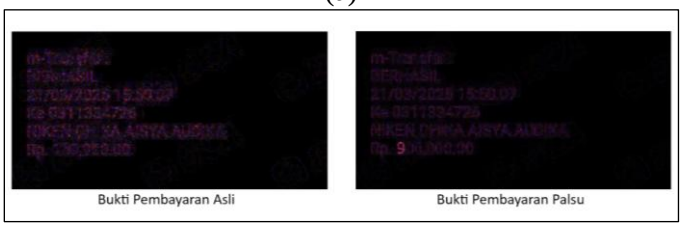
mengidentifikasi manipulasi pada bukti pembayaran digital, sementara implementasi dilakukan melalui aplikasi Android yang memungkinkan proses verifikasi dilakukan secara otomatis. Hasil menunjukkan bahwa integrasi teknologi forensik citra, OCR, dan KNN mampu meningkatkan akurasi deteksi serta efisiensi verifikasi dalam layanan keuangan digit

4.1 Pengujian

Proses pra-pemrosesan dilakukan untuk meningkatkan kualitas citra sebelum dianalisis lebih lanjut melalui tahapan OCR dan klasifikasi. Langkah ini bertujuan menyiapkan data visual secara optimal agar sistem mampu mengenali serta membedakan bukti pembayaran yang valid dan tidak valid.

Gambar 3 menunjukkan hasil tahapan pra-pemrosesan terhadap citra bukti pembayaran. Pada Gambar 3 bagian (a), ditampilkan contoh citra asli berupa tangkapan layar dari aplikasi *mobile banking*. Citra tersebut berisi elemen penting transaksi seperti nama pengirim, nominal transfer, tanggal, dan penerima, yang menjadi fokus dalam proses validasi keaslian. Gambar 3 bagian (b) menampilkan hasil ekstraksi citra setelah melalui serangkaian proses pra-pemrosesan, antara lain konversi ke skala keabuan (*grayscale*), binarisasi dengan metode *Otsu* untuk pemisahan teks dari latar belakang, pengurangan *noise* menggunakan median filter, serta koreksi orientasi (*deskewing*) untuk memastikan teks terbaca secara horizontal. Hasil akhir ini digunakan sebagai input dalam proses ekstraksi fitur tekstual melalui OCR dan selanjutnya diklasifikasikan menggunakan algoritma *K-Nearest Neighbor* (KNN).

(a)



(b)

Gambar 3 Pra-pemrosesan data (a) data bukti pembayaran (b) hasil ekstraksi bukti pembayaran

Dataset digunakan sebanyak 160 sampel hasil ekstraksi bukti pembayaran digital yang diperoleh melalui proses Optical Character Recognition (OCR). Data tersebut dibagi dengan rasio 80:20, menghasilkan 128 data sebagai data pelatihan dan 32 data sebagai data pengujian. Distribusi kelas antara bukti pembayaran asli dan tidak asli tetap seimbang sebelum dan sesudah proses pembagian. Model K-Nearest Neighbor (KNN) kemudian dilatih menggunakan data pelatihan dan diuji terhadap data pengujian, dengan hasil akurasi awal sebesar 53,19%. Hasil tersebut menunjukkan bahwa model memerlukan optimasi lebih lanjut untuk memperoleh performa klasifikasi yang lebih baik.

Proses pelatihan model dilakukan dengan menerapkan algoritma KNN untuk mengklasifikasikan keaslian bukti pembayaran digital berdasarkan hasil ekstraksi fitur tekstual. Berbagai nilai parameter k diuji guna menentukan nilai optimal dalam klasifikasi. Evaluasi dilakukan menggunakan metrik akurasi, presisi, recall, dan F1-score.

Berdasarkan hasil evaluasi, akurasi model meningkat secara signifikan seiring kenaikan nilai k hingga mencapai titik optimal. Hal ini menunjukkan bahwa nilai k yang lebih besar memungkinkan algoritma mempertimbangkan lebih banyak tetangga terdekat dalam menentukan kelas, sehingga memperkuat kemampuan model dalam mengenali pola-pola pada bukti pembayaran digital. Namun demikian, nilai k yang terlalu besar dapat menyebabkan penurunan akurasi karena adanya pengaruh noise dari data lain yang tidak relevan.

 ISSN:2302-8149
e-ISSN:2540-9719

Nilai *k* = 1 menghasilkan akurasi sebesar 93,62%, namun model menunjukkan sensitivitas yang tinggi terhadap outlier, sehingga mengurangi stabilitas performa dalam proses klasifikasi. Sementara itu, pada nilai *k* = 7, model mencapai performa optimal dengan akurasi sebesar 97,16%, presisi 97,10%, dan F1-score sebesar 97,10%. Hasil evaluasi menunjukkan bahwa performa model relatif stabil pada kisaran nilai k menengah. Sebaliknya, peningkatan nilai k secara berlebihan justru menurunkan akurasi akibat adanya pengaruh dari data tetangga yang kurang relevan atau berasal dari kelas berbeda. Berdasarkan hasil tersebut, nilai k = 7 ditetapkan sebagai parameter optimal karena mampu memberikan keseimbangan terbaik antara kemampuan generalisasi dan sensitivitas model dalam mengidentifikasi keaslian bukti pembayaran digital. Rincian lengkap hasil pengujian pada berbagai nilai *k* disajikan pada Tabel 2.

Tabel 2 menampilkan hasil pengujian model K-Nearest Neighbor (KNN) pada berbagai nilai *k* untuk menentukan parameter optimal dalam proses klasifikasi keaslian bukti pembayaran digital. Berdasarkan tabel tersebut, terlihat bahwa performa model mengalami peningkatan seiring bertambahnya nilai *k* hingga mencapai titik optimal pada *k* = 7 dengan nilai akurasi, presisi, recall, dan *F1-score* masing-masing sebesar 97,10%. Setelah melewati nilai tersebut, performa model cenderung menurun secara gradual akibat pengaruh data tetangga yang kurang relevan. Hasil ini menunjukkan bahwa pemilihan nilai *k* yang tepat berperan penting dalam menjaga keseimbangan antara sensitivitas dan kemampuan generalisasi model dalam mendeteksi keaslian bukti pembayaran digital.

Tabel 2 Hasil pelatihan model KNN

Nilai *k*	Akurasi	Presisi	*Recall*	*F1-Score*
1	0.9362	0.9412	0.9275	0.9343
2	0.9291	0.9275	0.9275	0.9275
3	0.9149	0.9014	0.9275	0.9143
4	0.9149	0.9130	0.9130	0.9143
5	0.9362	0.9412	0.9275	0.9343
6	0.9362	0.9286	0.9420	0.9353
7	0.9710	0.9710	0.9710	0.9710
8	0.9645	0.9706	0.9565	0.9635
9	0.9504	0.9559	0.9420	0.9489
10	0.9574	0.9701	0.9420	0.9559
11	0.9504	0.9559	0.9420	0.9489
12	0.9504	0.9559	0.9420	0.9489
13	0.9645	0.9571	0.9710	0.9640
14	0.9574	0.9565	0.9565	0.9565
15	0.9433	0.9420	0.9420	0.9420

4.2 Implementasi

Implementasi sistem dilakukan melalui aplikasi Android yang dirancang untuk mendeteksi keaslian bukti transfer digital secara otomatis menggunakan pendekatan image forensics dengan algoritma *K-Nearest Neighbor* (KNN). Aplikasi ini dibangun dengan antarmuka sederhana agar memudahkan pengguna dalam melakukan proses validasi. Fitur navigasi aplikasi mencakup tombol Upload Bukti untuk memulai proses baru, serta Data Transaksi untuk melihat riwayat validasi yang telah dilakukan.

Pada Gambar 4 menampilkan antarmuka aplikasi pada tahap verifikasi bukti pembayaran digital. Pada bagian ini, pengguna dapat memilih fitur “Upload Bukti” untuk mengunggah citra bukti transfer melalui kamera atau galeri perangkat. Setelah citra diunggah, sistem secara otomatis melakukan ekstraksi ciri visual dan analisis klasifikasi menggunakan model *K-Nearest Neighbor* (KNN) untuk menentukan status keaslian bukti. Pada tampilan ini, antarmuka dirancang sederhana dan interaktif

 ISSN:2302-8149
e-ISSN:2540-9719

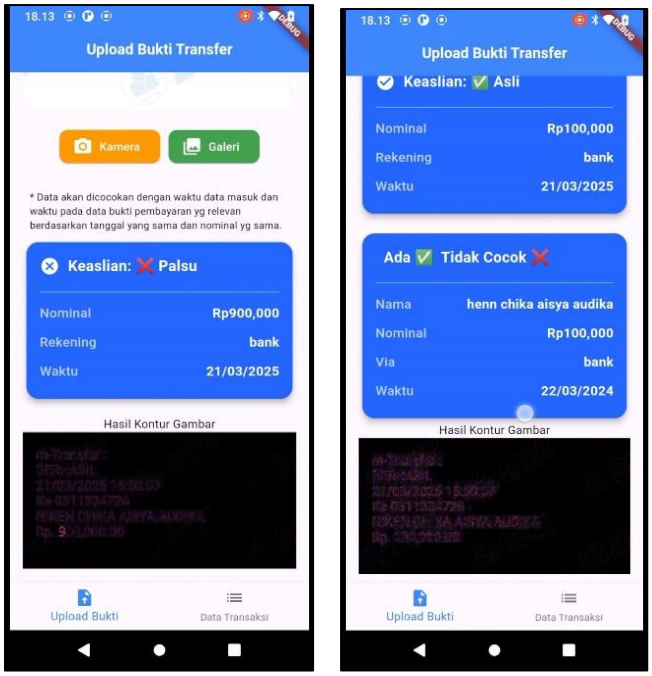
agar pengguna dapat melakukan unggahan serta memperoleh hasil verifikasi dengan cepat dan mudah dipahami.

Gambar 4 Tampilan aplikasi

Setelah proses analisis selesai, aplikasi akan menampilkan hasil klasifikasi keaslian bukti transfer pada antarmuka pengguna.. Hasil terdiri dari dua bagian utama, yaitu:

1. Status Keaslian
   Sistem akan mengklasifikasikan bukti transfer sebagai Asli atau Palsu , berdasarkan perhitungan algoritma terhadap fitur citra. Contoh hasil klasifikasi menunjukkan bukti dinyatakan Asli, ditandai dengan teks “Keaslian: Asli”.
2. Pencocokan Data Transfer
   Selain status keaslian, sistem juga membandingkan hasil ekstraksi teks dengan data transaksi yang ada. Informasi yang dibandingkan meliputi nama pengirim, nominal, metode pengiriman (via rekening/bank), dan waktu transaksi. Jika terdapat ketidaksesuaian, sistem akan memberikan indikator Tidak Cocok meskipun keaslian bukti valid. Hal ini untuk mendeteksi kemungkinan pemalsuan informasi meskipun gambar transfer asli.

 ISSN:2302-8149
e-ISSN:2540-9719



Gambar 5. Tampilan hasil validasi dan pencocokan data

Pada Gambar 5 menampilkan hasil akhir proses verifikasi yang mencakup dua komponen utama, yaitu status keaslian bukti transfer dan pencocokan data transaksi. Pada bagian bawah antarmuka aplikasi juga ditampilkan "Hasil Kontur Gambar", yang merepresentasikan proses ekstraksi visual terhadap citra bukti transfer. Kontur tersebut berfungsi sebagai bukti pendukung bahwa sistem benar-benar melakukan analisis terhadap struktur citra, bukan semata-mata membaca teks hasil ekstraksi. Melalui tampilan ini, pengguna dapat melihat visualisasi proses analisis yang dilakukan oleh sistem, sehingga memberikan transparansi dan keandalan dalam proses verifikasi. Dengan adanya fitur ini, aplikasi mampu melakukan validasi keaslian serta konsistensi data bukti transfer digital secara otomatis, cepat, dan efisien dalam konteks sistem pembayaran elektronik maupun audit transaksi.

5 Kesimpulan

Berdasarkan hasil penelitian ini, dapat disimpulkan bahwa proses identifikasi dan validasi keaslian bukti pembayaran digital dapat dilakukan secara otomatis melalui integrasi *teknologi Image Processing*, *Image Forensics*, dan *Optical Character Recognition* (OCR). Pendekatan terpadu ini memungkinkan sistem mendeteksi manipulasi digital pada citra, mengekstraksi informasi teks dengan OCR, serta menganalisis keaslian data pembayaran secara komprehensif. Teknologi *Image Processing* meningkatkan kualitas visual, *Image Forensics* mengungkap jejak rekayasa digital, dan OCR mentransformasikan informasi menjadi teks yang dapat dianalisis oleh sistem klasifikasi. Pada tahap klasifikasi, algoritma *K-Nearest Neighbor* (KNN) digunakan dan menunjukkan performa optimal pada nilai $k = 7$ dengan akurasi 97,16%, presisi 97,10%, recall 97,10%, dan *F1-score* 97,10%. Variasi format citra, perbedaan resolusi, kualitas pencahayaan, serta hasil OCR yang dipengaruhi oleh kejernihan dan kemiringan teks menjadi tantangan dalam menjaga konsistensi performa sistem. Oleh karena itu, keberhasilan sistem sangat ditentukan oleh efektivitas tahapan pra-pemrosesan dan pemilihan parameter klasifikasi yang tepat. Secara keseluruhan, penelitian ini menunjukkan bahwa pendekatan berbasis forensik citra dan teks memiliki potensi besar dalam memperkuat sistem verifikasi otomatis, khususnya dalam mendukung efisiensi dan keamanan transaksi pada layanan keuangan digital.

Referensi

[1] H. H. Nawawi, "Penggunaan *E-Wallet* di Kalangan Mahasiswa," *Emik*, Vol. 3, No. 2, pp. 189–205, 2020.
[2] G. Newswire, "*Fraud and Security in Global Online Payments Market 2024 – Global B2C E-*

 ISSN:2302-8149
e-ISSN:2540-9719

Commerce Fraud Losses to Grow by +40% CAGR from 2023 to 2028," *Fintech Futures*, 2024. .

[3] N. Dekker, "*Staggering Payment Fraud Statistics You Need to Know*," *Eftsure*, 2025. .

[4] Alfin Fanther, "*QRIS: Indonesia's Financial Technology that Shakes the World*," *Medium*, 2025. .

[5] H. Mulyawan, M. Z. H. Samsono, and Setiawardhana, "Identifikasi dan *Tracking* Objek berbasis *Image*," Identifikasi dan *Track. Objek berbasis Image Process. Secara Real Time*, pp. 1–5, 2011, [Online]. Available: http://repo.pens.ac.id/1324/1/Paper_TA_MBAH.pdf.

[6] L. A. Permana, F. Hakim, Y. A. Subhi, and P. Rivaldo, "Analisis Forensik Keaslian Gambar menggunakan *Autopsy*," *J. JOCOTIS-Journal SCI. Inform. Robot. E*, Vol. 1, No. 2, pp. 39–45, 2023, [Online]. Available: https://jurnal.ittc.web.id/index.php/jct/.

[7] S. Muharom, "Pengenalan Nomor Ruangan menggunakan Kamera berbasis OCR dan *Template Matching*," *Inf. J. Ilm. Bid. Teknol. Inf. dan Komun.*, Vol. 4, No. 1, pp. 28–32, 2019, DOI: 10.25139/inform.v3i2.1010.

[8] I. Irwansyah and H. Yudiastuti, "Analisis Digital Forensik Rekayasa *Image* menggunakan *Jpegsnoop* dan *Forensically* Beta," *J. Ilm. Matrik*, Vol. 21, No. 1, pp. 54–63, 2019, DOI: 10.33557/jurnalmatrik.v21i1.518.

[9] H. A. Raheem, M. A. Mohammed, and A. S. H. M. Ali, "*Enhancing the Image Forgery Detection based Machine Learning Approach using Multiple Datasets*," *Eng. Technol. Appl. Sci. Res.*, Vol. 15, No. 3, pp. 22739–22745, 2025.

[10] E. Nowroozi, A. Dehghantanha, R. M. Parizi, and K.-K. R. Choo, "*A Survey of Machine Learning Techniques in Adversarial Image Forensics*," *Comput. Secur.*, Vol. 100, p. 102092, 2021.

[11] I. T. Ahmed, B. T. Hammad, and N. Jamil, "*Forgery Detection Algorithm based on Texture Features*," *Indones. J. Electr. Eng. Comput. SCI.*, Vol. 24, No. 1, pp. 226–235, 2021.

[12] E. A. L. M. Btoush, X. Zhou, R. Gururajan, K. C. Chan, R. Genrich, and P. Sankaran, "*A Systematic Review of Literature on Credit Card Cyber Fraud Detection using Machine and Deep Learning*," *PeerJ Comput. SCI.*, Vol. 9, p. e1278, 2023.

[13] Ajay N. Upadhyaya, "*Enhancing Credit Card Fraud Detection with K-Nearest Neighbours (KNN): A Machine Learning Approach*," *J. Inf. Syst. Eng. Manag.*, Vol. 10, No. 2, pp. 498–506, 2025, DOI: 10.52783/jisem.v10i2.2388.

[14] N. Malini and M. Pushpa, "*Investigation of Credit Card Fraud Recognition Techniques based on KNN and HMM*," in *IJCA Proceedings on International Conference on Communication, Computing and Information Technology ICCCMIT*, 2017, Vol. 1, pp. 9–13.

[15] S. A. Wibowo and K. Usman, "*Voice Activity Detection G729B Improvement Technique using K-Nearest Neighbor Method*," *2010 Int. Conf. Distrib. Fram. Multimed. Appl. DFmA 2010*, No. January 2010, 2010, DOI: 10.13140/2.1.4362.5764.