



Analisis Penerapan Error Level Analysis (ELA) Terintegrasi CNN untuk Deteksi Manipulasi Video dalam Digital Forensik

Yahya Sarifudin¹, Yudi Prayudi²

^{1,2}Universitas Islam Indonesia

E-mail: yahyasarifudin@gmail.com

Article Info	Abstract
Article History Received: 2025-12-08 Revised: 2026-01-15 Published: 2026-02-12 Keywords: ELA; Error Level Analysis; CNN; Convolution Neural Network.	There has been an increase in visual-based digital content or works, both images and videos, making them valuable digital assets. However, the ease of access and the development of various manipulation tools and techniques have opened up opportunities for crime by exploiting this type of video manipulation. To minimize the impact of disinformation and misinterpretation, and to safeguard and protect intellectual property from manipulation, strategies are needed to maintain authenticity. Authenticity identification mechanisms without the aid of specialized scientific tools or methods create the potential for misinterpretation. One method or step to detect manipulation is ELA. The implementation of the Error Level Analysis (ELA) method in video forensics for detecting video manipulation uses a case study scheme by testing a manipulated video dataset. Experimental analysis of the implementation of this ELA method is integrated with other models, such as the CNN algorithm with SVM and KNN techniques, or thresholds that have been proven to detect image manipulation. The results of the deep fake manipulation detection achieved an accuracy of 54%. The model cannot yet identify real and fake videos.
Artikel Info	Abstrak
Sejarah Artikel Diterima: 2025-12-08 Direvisi: 2026-01-15 Dipublikasi: 2026-02-12 Kata kunci: ELA; Error Level Analysis; CNN; Convolution Neural Network.	Terjadi peningkatan konten atau karya digital berbasis visual baik gambar ataupun video, karya atau konten menjadi aset digital berharga. Namun kemudahan akses dan berkembangnya berbagai <i>tools</i> dan teknik manipulasi, membuka peluang kejahatan dengan memanfaatkan jenis manipulasi video. Untuk meminimalisir dampak disinformasi, misinterpretasi, menjaga, dan melindungi kekayaan intelektual dari manipulasi perlu strategi untuk mempertahankan keaslian. Mekanisme identifikasi keaslian tanpa bantuan <i>tools</i> atau metode khusus secara <i>scientific</i> menimbulkan peluang misinterpretasi. Salah satu metode atau langkah-langkah untuk mendeteksi manipulasi adalah ELA. Implementasi metode <i>Error Level Analysis (ELA)</i> dalam video forensik untuk deteksi manipulasi video menggunakan skema studi kasus dengan melakukan pengujian terhadap <i>dataset</i> video manipulasi. Analisis eksperimen implementasi metode ELA ini, diintegrasikan dengan model lain misalnya algoritma CNN dengan teknik SVM dan KNN atau <i>threshold</i> yang telah terbukti untuk deteksi manipulasi gambar. Hasil deteksi manipulasi <i>deep fakes</i> memperoleh hasil <i>accuracy</i> sebesar 54%. Model belum bisa mengidentifikasi video <i>Real</i> dan <i>Fake</i> .

I. PENDAHULUAN

Informasi yang berkaitan dengan pelanggaran atau perilaku melanggar hukum, termasuk namun tidak terbatas pada penyebaran tipuan atau penyebaran informasi yang menyesatkan sebagaimana diuraikan dalam Undang-Undang Informasi dan Transaksi Elektronik (ITE), menunjukkan tren kenaikan yang terlihat dalam frekuensi dan tingkat keparahan pelanggaran tersebut. Kesimpulan ini didukung oleh analisis komprehensif dari jumlah agregat penyelidikan yang dilakukan di situs web resmi terkait dengan putusan Mahkamah Agung, yang mengungkapkan total signifikan 1.314 pencarian yang dicatat hingga tahun ini. Tercatat pelanggaran UU ITE di semua tempat atau daerah Pengadilan. Mahkamah Agung sebesar 44 pelanggaran.

Selanjutnya PN Jakarta Selatan sebesar 31. Kemudian disusul Pengadilan Negeri Denpasar sebesar 25, PA Jakarta selatan sebesar 24, PA Cikarang sebesar 22, PT medan sebesar 18. Tercatat klasifikasi putusan terkait dengan ITE menempati posisi paling banyak yaitu sejumlah 436. Seiring meningkatnya pelanggaran UU ITE, Peningkatan produksi dan konsumsi konten digital berbasis visual seperti gambar dan video, menjadi tantangan dalam menjaga keaslian (Yallamandhala & Godwin, 2022) dan integritas aset digital yang semakin kompleks.

Berbagai teknik manipulasi semakin canggih, memungkinkan penyalahgunaan konten untuk tujuan disinformasi, pemalsuan identitas, dan kejahatan digital lainnya. (Mohiuddin et al., 2023) salah satu bukti digital/elektronik adalah

video, didalamnya kemungkinan terdapat pelanggaran hukum / tindak pidana yang menyangkut dengan pencemaran nama baik/ berita bohong. Tercatat data statistik dari situs patroli siber paling banyak ke-3 adalah kasus pencemaran nama baik. Diperlukan metode yang efektif dalam mendeteksi manipulasi agar dapat memastikan keabsahan suatu konten digital. Salah satu teknik yang digunakan dalam mendeteksi manipulasi citra digital adalah Error Level Analysis (ELA). Metode ini bekerja dengan menganalisis tingkat kesalahan kompresi pada suatu gambar untuk mengidentifikasi potensi perubahan yang menunjukkan adanya manipulasi (Farook, 2024; Raković, 2023)

Studi sebelumnya menunjukkan bahwa ELA mampu mendeteksi pemalsuan gambar dengan akurasi tinggi (R. Gorle and A. Guttavelli, 2025), mencapai 89,5% dalam berbagai eksperimen (CPatel & M Patel, 2015; Patel & Patel, 2015) (Idlbek et al., 2024; Rafique et al., 2021; Verma et al., 2024) Namun, mayoritas penelitian yang ada masih berfokus pada manipulasi gambar dengan format JPEG dan terbatas pada teknik seperti *splicing*, *copy-move forgery*, dan *retouching* (T. Sari et al., 2016). Seiring dengan meningkatnya kompleksitas manipulasi digital, pemalsuan tidak hanya terjadi pada gambar statis tetapi juga pada konten video (Harika Palivela et al., 2023). Beberapa teknik manipulasi video yang umum digunakan meliputi *copy-move*, *splicing* (H. Kaur & Jindal, 2020), serta penggunaan teknologi *deepfake* (A. Kaur et al., 2024).

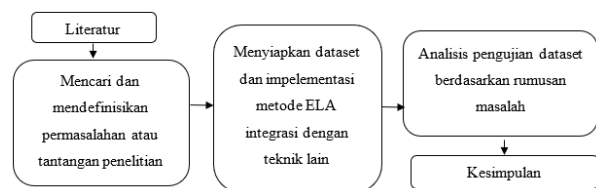
Sayangnya, meskipun metode ELA telah terbukti efektif dalam mendeteksi manipulasi gambar, penerapannya pada analisis video forensik masih menghadapi tantangan yang signifikan. Beberapa studi awal menunjukkan bahwa efektivitas ELA dalam mendeteksi manipulasi video sangat dipengaruhi oleh kualitas video, jenis manipulasi yang digunakan, parameter ELA yang diterapkan, serta karakteristik objek bergerak dan efek visual dalam video (Jeronymo et al., 2017; Warif et al., 2015) atau kasus spesifik (Mohiuddin et al., 2023). Penelitian lainnya telah mencoba meningkatkan akurasi deteksi manipulasi gambar dengan mengombinasikan ELA dengan algoritma pembelajaran mesin seperti *Convolutional Neural Network* (CNN) (Mohammed et al., 2024; Vasudevan et al., 2025), *Support Vector Machine* (SVM), dan *K-Nearest Neighbors* (KNN) (Rafique et al., 2021, 2023; W. P. Sari & Fahmi, 2021; Verma et al., 2024). (Mercier et al., 2019; Nagm et al., 2024)

Pendekatan ini menunjukkan peningkatan akurasi dalam mendeteksi manipulasi gambar, namun implementasi serupa pada video masih perlu dieksplorasi lebih lanjut (Sandhya & Kashyap, 2024). (More et al., 2024; Panchal & Shah, 2020) Oleh karena itu, terdapat kebutuhan mendesak untuk mengembangkan strategi optimasi ELA agar dapat digunakan secara efektif dalam analisis video forensik.

Berdasarkan research gap tersebut, penelitian ini bertujuan untuk implementasi metode ELA dalam mendeteksi manipulasi video, mengidentifikasi faktor-faktor yang mempengaruhi akurasi, serta mengembangkan strategi optimasi untuk meningkatkan kinerja metode. Hasil dari penelitian ini diharapkan dapat memberikan kontribusi dalam pengembangan teknik analisis video forensik yang lebih akurat dan andal.

II. METODE PENELITIAN

Penelitian ini menggunakan pendekatan studi kasus atau eksperimental dengan menganalisis dataset atau melakukan pengujian, adapun tahapan atau langkah-langkah untuk melakukan penelitian sebagai berikut :

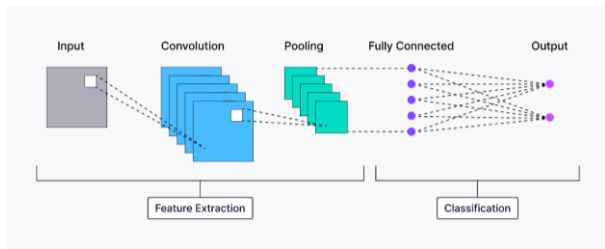


Gambar 1. Langkah-Langkah Penelitian

Berdasarkan Gambar 1 Langkah-Langkah Penelitian tahap awal terdapat Literatur yang mana melakukan studi literatur dari penelitian terdahulu terkait dengan deteksi manipulasi video menggunakan metode ELA dan integrasi CNN. Hasil penelitian terdahulu dirangkum kemudian diidentifikasi permasalahan atau tantangan penelitian. Berdasarkan hasil identifikasi terdapat tantangan penelitian khususnya untuk deteksi manipulasi untuk konteks video. Adapun teknik manipulasi video ada beberapa teknik manipulasi berikut:

1. *Copy Move* adalah teknik manipulasi gambar dengan cara menyalin sebagian gambar dan ditempel di tempat lain dalam gambar yang sama.
2. *Splicing* adalah teknik manipulasi gambar dengan cara memindahkan objek gambar ke gambar lain
3. *Deep Fake* adalah gambar, video atau audio yang telah diedit atau dihasilkan menggunakan kecerdasan buatan atau alat

berbasis AI, atau perangkat lunak penyunting audio-video.



Gambar 2. Arsitektur CNN

Gambar 2 Arsitektur CNN, lapisan pertama pada Convolutional Neural Network merupakan lapisan input yang diproses melalui lapisan konvolusi (*convolution layer*) untuk mengekstraksi fitur awal dari citra. Selanjutnya, hasil konvolusi tersebut dilewatkan ke lapisan subsampling (*pooling*) berukuran 2×2 , yang berfungsi untuk mengurangi dimensi fitur sekaligus mempertahankan informasi penting.

Proses ini kemudian diikuti oleh lapisan konvolusi berukuran kernel 5×5 yang bertujuan mengekstraksi fitur yang lebih kompleks, dilanjutkan kembali dengan lapisan subsampling 2×2 . Rangkaian lapisan konvolusi dan subsampling tersebut dikategorikan sebagai tahap *feature extraction*, karena berfungsi untuk menangkap pola visual, tekstur, dan struktur penting pada citra.

Setelah proses ekstraksi fitur selesai, fitur yang dihasilkan diratakan (*flatten*) dan diteruskan ke lapisan *fully connected*, yang berperan sebagai tahap *classification* untuk menentukan kelas atau label dari data masukan berdasarkan fitur yang telah dipelajari.

III. HASIL DAN PEMBAHASAN

A. Hasil Penelitian

Analisis video forensic adalah dengan metode scientific merekonstruksi khususnya untuk mendeteksi manipulasi pada konten video khususnya untuk jenis manipulasi *deep fakes*.

Pertama import library yang dibutuhkan seperti `numpy`, `torch`, `torchvision`, `ImageChrops`, `ImageDraw` dst.

Penelitian ini menggunakan pendekatan studi eksperimental dengan melakukan pengujian metode Error Level Analysis (ELA) pada dataset video forensic yang mengandung berbagai jenis manipulasi. Langkah-langkah penelitian yang dilakukan meliputi:

1. Tahap Pengumpulan Data

Dataset yang digunakan adalah kumpulan video yang mengandung

manipulasi seperti *copy-move*, *forgery*, *splicing*, dan *deep fakes* dari sumber dataset publik, seperti:

a) Video Forgery Detection Dataset (Dataset *Video Forged and Original*, n.d.)

b) Kaggle: Dataset manipulasi video terkait forensik digital. (*Deep Fake Detection (DFD) Entire Original Dataset*, n.d.)

Dataset yang digunakan dalam penelitian ini diperoleh dari platform Kaggle, dengan total ukuran sekitar 19,8 GB untuk video hasil manipulasi (manipulated/deepfake videos) dan 2,7 GB untuk video asli (original videos). Secara keseluruhan, dataset tersebut menyediakan cakupan data yang cukup besar dan beragam untuk mendukung penelitian deteksi deepfake.

Namun demikian, dalam praktiknya, penggunaan seluruh dataset tidak dapat dilakukan secara langsung karena adanya keterbatasan sumber daya komputasi, khususnya kapasitas memori (RAM dan/atau GPU memory) pada perangkat yang digunakan. Ketika seluruh data dimuat dan diproses secara bersamaan, sistem mengalami kendala memori yang menyebabkan kegagalan proses pelatihan dan inferensi.

Oleh karena itu, penelitian ini menggunakan sub-sampel dataset yang diambil secara selektif dari keseluruhan data yang tersedia. Sub-sampel tersebut diekstraksi dalam bentuk frame video dan disesuaikan dengan kapasitas perangkat, sehingga proses pelatihan dan evaluasi model dapat berjalan secara stabil. Meskipun ukuran data yang digunakan lebih kecil dibandingkan dataset awal, pendekatan ini tetap memungkinkan model untuk mempelajari pola artefak manipulasi yang relevan.

Keterbatasan ini dicatat sebagai batasan penelitian (*research limitation*) dan menjadi dasar untuk pengembangan lebih lanjut di masa mendatang, khususnya dengan dukungan perangkat keras yang lebih memadai atau strategi pemrosesan data yang lebih efisien, seperti streaming data, batch processing, atau pelatihan terdistribusi.

2. Preprocessing Data

Berdasarkan Tabel 4.1 Data Total Video, Dataset yang digunakan dalam penelitian ini terdiri dari 101 video dengan total

3.381 frame hasil ekstraksi. Dari jumlah tersebut, 50 frame merupakan kelas real, sedangkan 3.331 frame termasuk dalam kelas fake. Seluruh frame memiliki ukuran 224×224 piksel dengan 3 kanal warna (RGB).

Untuk mengatasi ketidakseimbangan kelas (*class imbalance*) yang signifikan antara kelas real dan fake, diterapkan class weighting pada proses pelatihan model. Bobot kelas yang digunakan adalah 33,81 untuk kelas real (0) dan 0,51 untuk kelas fake (1).

Tabel 1. Dataset Trinin

Jumlah Video	Total Frame	Real Frame	Fake Frame	Frame Shape	Class Weight
101	3,381	50	3,331	3381, 224, 3	0:np.float64(33.81) 1:np.float64(0.5075052536775743)

B. Pembahasan

1. Tahap Implementasi Metode ELA

Fungsi *apply_ela* dirancang untuk menerapkan metode Error Level Analysis (ELA) pada sebuah frame citra. Fungsi ini bersifat fleksibel dan dapat dipanggil secara modular dalam berbagai tahapan pemrosesan, termasuk sebelum proses inialisasi deteksi menggunakan model CNN.

Proses ELA diawali dengan normalisasi nilai piksel dari frame masukan. Apabila frame memiliki rentang nilai antara 0 hingga 1, nilai tersebut dikonversi kembali ke rentang 0 hingga 255 untuk memastikan format citra sesuai dengan standar kompresi lossy. Selanjutnya, data citra dinormalisasi ke tipe uint8 agar dapat dikompresi secara valid menggunakan algoritma JPEG.

Frame kemudian dikonversi dari format NumPy array ke objek PIL Image untuk keperluan kompresi. Citra tersebut disimpan sementara menggunakan kompresi lossy JPEG dengan tingkat kualitas sebesar 95%, yang bertujuan untuk dapat mempertahankan detail visual utama sambil tetap memunculkan perbedaan tingkat kompresi.

Setelah proses kompresi, perbedaan nilai piksel antara citra asli dan citra hasil kompresi dihitung. Selisih ini merepresentasikan tingkat kesalahan kompresi pada setiap piksel, yang sering kali menonjol pada area yang mengalami manipulasi.

Perbedaan tersebut kemudian diperkuat dengan meningkatkan kontras pencahayaan hingga mencapai skala maksimum agar artefak manipulasi menjadi lebih jelas terlihat.

Setelah proses peningkatan perbedaan selesai, berkas citra sementara dihapus untuk menjaga efisiensi penyimpanan. Terakhir, citra hasil ELA yang telah diperkuat dikonversi kembali ke format NumPy array, sehingga siap digunakan sebagai masukan bagi tahapan pemrosesan selanjutnya atau langsung diberikan ke model CNN.

2. Tahap Optimasi dan Pengembangan Model CNN

Arsitektur CNN pada kelas AdvancedDeepfakeDetector dirancang untuk meningkatkan stabilitas pelatihan dan sensitivitas terhadap artefak halus yang umum ditemukan pada konten deepfake. Model ini mengintegrasikan beberapa mekanisme utama sebagai berikut:

a) Residual Connections

Model ini menerapkan residual connections (skip connections) pada beberapa blok konvolusional. Mekanisme ini memungkinkan aliran gradien yang lebih stabil selama proses pelatihan, sehingga membantu mengurangi permasalahan vanishing gradients serta mempercepat konvergensi pada jaringan yang relatif dalam.

b) Attention Mechanism (Channel-wise Attention)

Model mengadopsi mekanisme channel-wise attention yang diimplementasikan melalui rangkaian Global Average Pooling → Dense → Dense → Multiply. Mekanisme ini memungkinkan jaringan untuk menyesuaikan bobot pada setiap kanal fitur berdasarkan tingkat kepentingannya, sehingga model dapat lebih fokus pada fitur-fitur informatif yang berkaitan dengan artefak manipulasi halus pada deepfake. Pendekatan ini sangat relevan untuk tugas forensik digital yang menuntut sensitivitas tinggi terhadap perbedaan tekstur dan pola kompresi.

c) Regularization

Untuk mengurangi risiko overfitting, model menerapkan beberapa teknik regularisasi, yaitu Dropout pada

berbagai tahap jaringan dan regularisasi kernel L2 pada lapisan konvolusional dan dense. Kombinasi ini membantu membatasi kompleksitas model sekaligus meningkatkan kemampuan generalisasi, terutama pada dataset berukuran terbatas.

d) Dual Pooling Strategy

Sebelum memasuki lapisan fully connected, model menggabungkan Global Average Pooling (GAP) dan Global Max Pooling (GMP). Strategi dual pooling ini memungkinkan model menangkap informasi distribusi fitur global sekaligus respons aktivasi ekstrem, yang penting untuk dapat mendeteksi inkonsistensi lokal maupun global pada citra deepfake.

e) Metrik Evaluasi

Kinerja model dievaluasi menggunakan serangkaian metrik yang komprehensif, meliputi Accuracy, Area Under the ROC Curve (AUC), Precision, Recall, dan Binary Accuracy. Kombinasi metrik ini memberikan gambaran yang lebih menyeluruh terhadap performa klasifikasi, khususnya dalam konteks dataset yang berpotensi tidak seimbang antara kelas asli dan deepfake.

3. Trining Model

Model dilatih untuk mempelajari pola dan hubungan antara fitur-fitur yang diekstraksi dari frame video. Dataset dibagi menjadi 3.944 sampel pelatihan dan 987 sampel pengujian, yang memberikan proporsi data uji yang memadai untuk evaluasi performa akhir model. Pelatihan dilakukan selama 30 epoch, jumlah yang umumnya cukup untuk mengamati proses konvergensi model.

Namun, mengingat ukuran dataset yang relatif terbatas, terdapat risiko overfitting sehingga diperlukan pemantauan kinerja validasi secara cermat. Ukuran batch sebesar 16 dipilih karena batch yang lebih kecil menghasilkan lebih banyak pembaruan bobot per epoch, yang sering kali membantu meningkatkan kemampuan generalisasi model, khususnya pada dataset berukuran kecil hingga menengah. Sebanyak 15% dari data pelatihan (sekitar 592 sampel) digunakan sebagai data validasi.

Pembagian ini memungkinkan pemantauan performa model selama proses

pelatihan tanpa melibatkan data uji, sehingga evaluasi akhir tetap objektif. Dengan ukuran batch 16, setiap epoch terdiri dari sekitar 247 langkah pelatihan (3944 / 16).

Model yang digunakan memiliki sekitar 6,5 juta parameter, yang tergolong cukup besar untuk dataset ini namun masih berada pada keseimbangan yang wajar antara kapasitas representasi dan efisiensi komputasi.

Oleh karena itu, penerapan teknik regularisasi seperti dropout dan regularisasi L2 menjadi sangat penting untuk mengurangi risiko overfitting dan meningkatkan stabilitas pelatihan. Secara keseluruhan, konfigurasi pelatihan ini dirancang untuk memberikan kompromi yang baik antara kekuatan model dan keterbatasan jumlah data, dengan tetap menjaga validitas evaluasi melalui pemisahan data pelatihan, validasi, dan pengujian.

Fungsi *train()* digunakan untuk melatih model CNN dengan memanfaatkan teknik augmentasi data dan mekanisme early stopping untuk meningkatkan kemampuan generalisasi. Data pelatihan diberikan dalam bentuk frame video beserta labelnya, sementara data uji disimpan terpisah dan hanya digunakan untuk evaluasi akhir.

Selama proses pelatihan, data pelatihan dibagi lebih lanjut menjadi data latih dan data validasi menggunakan rasio *validation_split*. Augmentasi data diterapkan melalui ImageDataGenerator dengan transformasi geometris ringan seperti rotasi, pergeseran, pembesaran, dan horizontal flipping untuk memperkaya variasi data dan mengurangi overfitting.

Proses pelatihan dipantau menggunakan beberapa callback, termasuk Early Stopping berbasis metrik AUC validasi, Reduce Learning Rate on Plateau untuk menyesuaikan laju pembelajaran secara adaptif, serta Model Checkpoint untuk menyimpan model dengan performa validasi terbaik. Setelah pelatihan selesai, model dievaluasi menggunakan data uji yang tidak pernah disentuh selama proses pelatihan maupun validasi.

4. Integrasi ELA dengan Algoritma Kecerdasan Buatan

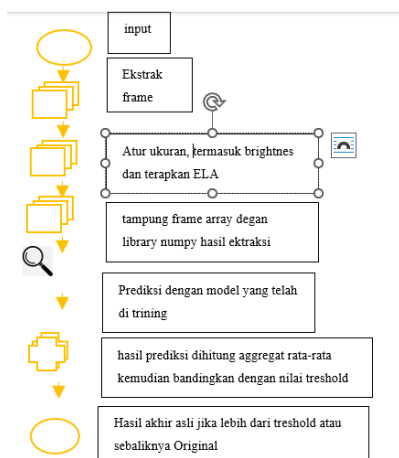
- Mengimplementasikan metode deep learning (CNN, SVM, atau KNN) untuk meningkatkan deteksi manipulasi.
- Model akan dilatih untuk mempelajari pola dan hubungan antara fitur-fitur.

Mekanisme peningkatan ELA dengan pendekatan CNN atau SVM or KNN untuk meningkatkan akurasi deteksi.

Integrasi metode ELA dengan CNN model untuk deteksi video manipulasi. Fungsi *preprocess_frame()* bertanggung jawab untuk melakukan pra-pemrosesan setiap frame video sebelum diberikan sebagai masukan ke model CNN. Frame yang diperoleh dari OpenCV umumnya berada dalam format warna BGR, sehingga langkah awal dilakukan konversi ke format RGB untuk memastikan konsistensi representasi warna.

Selanjutnya, frame diubah ukurannya menjadi dimensi tetap sesuai dengan kebutuhan input model, yaitu $img_size \times img_size$. Error Level Analysis (ELA) diaktifkan, frame yang telah diubah ukurannya akan diproses menggunakan metode ELA untuk mengekstraksi perbedaan tingkat kompresi, yang sering kali berkaitan dengan area manipulasi pada citra digital.

Tahap akhir pra-pemrosesan adalah normalisasi nilai piksel ke rentang [0, 1] dengan membagi nilai intensitas piksel dengan 255. Normalisasi ini membantu menstabilkan proses pelatihan dan inferensi jaringan saraf dengan memastikan skala input yang konsisten.



Gambar 3. Integrasi ELA dengan CNN

5. Deteksi Manipulasi

Fungsi *detect_manipulation()* digunakan untuk mendeteksi indikasi manipulasi pada sebuah video dengan melakukan inferensi berbasis frame. Proses diawali dengan validasi keberadaan dan format berkas video, kemudian dilanjutkan dengan ekstraksi frame menggunakan OpenCV.

Setiap frame yang diekstraksi diproses melalui fungsi *preprocess_frame()* agar sesuai dengan format input model CNN. Frame-frame yang telah diproses kemudian disusun menjadi sebuah array dan diberikan sebagai masukan ke model deep learning untuk menghasilkan skor probabilitas manipulasi pada tingkat frame.

Prediksi pada tingkat video diperoleh melalui agregasi statistik dari skor frame, meliputi:

Rata-rata skor (average score) sebagai indikator utama tingkat manipulasi video, Median skor untuk mengurangi pengaruh outlier, Simpangan baku (standard deviation) untuk mengukur konsistensi prediksi antar-frame, Persentase frame terdeteksi palsu berdasarkan ambang batas (threshold) yang ditentukan.

Keputusan akhir klasifikasi video ditentukan berdasarkan perbandingan nilai rata-rata skor dengan ambang batas klasifikasi. Selain itu, tingkat kepercayaan (confidence) dihitung sebagai jarak skor rata-rata terhadap ambang keputusan, yang merepresentasikan keyakinan model terhadap hasil klasifikasi. Pendekatan berbasis agregasi frame ini memungkinkan deteksi manipulasi yang lebih robust dibandingkan klasifikasi tunggal, khususnya pada video yang hanya mengalami manipulasi parsial atau temporer

6. Evaluasi dan Analisis Hasil

Menggunakan metrik evaluasi seperti Precision, Recall, F1-Score, dan AUC-ROC Curve.

Model yang telah dilatih kemudian diuji menggunakan dataset yang berbeda dari dataset pelatihan untuk mengevaluasi kemampuan generalisasi. Hasil pengujian menunjukkan bahwa performa model mengalami penurunan yang signifikan, dengan nilai akurasi sebesar 54%. Nilai ini mengindikasikan bahwa model masih menghasilkan tingkat kesalahan klasifikasi

yang cukup tinggi ketika dihadapkan pada distribusi data yang berbeda.

Grafik *Accuracy* menunjukkan nilai *train* pada epoch ke-6 sebesar 0,55 dan *validation* 0,35 menunjukkan model belum *generalize* dengan baik. Penyebab utama karena dataset terlalu kecil dan model terlalu sederhana.

Pada grafik *Loss*, pada epoch ke-6 terlihat adanya kesenjangan yang signifikan antara nilai *training loss* dan *validation loss*. Nilai *training loss* berada pada kisaran ≈ 1 , sedangkan *validation loss* meningkat tajam hingga ≈ 6 . Kondisi ini menunjukkan bahwa model mampu menyesuaikan diri dengan baik terhadap data pelatihan, namun gagal mempertahankan performa yang sama pada data validasi.

Pada grafik AUC (Area Under the Curve) terlihat bahwa pada epoch ke-6, nilai AUC data pelatihan (train) mencapai 0,57, sedangkan nilai AUC data validasi (validation) berada pada kisaran 0,50. Nilai AUC sebesar 0,50 pada data validasi menunjukkan bahwa kemampuan model dalam membedakan antara video asli dan video manipulasi pada data yang belum pernah dilihat masih setara dengan tebakan acak (*random guessing*).

Perbedaan nilai AUC antara data pelatihan dan data validasi mengindikasikan bahwa model mulai mempelajari pola pada data pelatihan, namun pola tersebut belum dapat digeneralisasikan dengan baik ke data validasi. Kondisi ini dapat disebabkan oleh keterbatasan jumlah dan keberagaman dataset pelatihan, serta kompleksitas artefak manipulasi video yang beragam. Nilai AUC pelatihan yang sedikit lebih tinggi (0,57) menunjukkan adanya peningkatan kemampuan diskriminatif model pada data yang digunakan untuk pelatihan. Namun, penurunan kinerja pada data validasi menandakan bahwa model belum cukup stabil dan masih rentan terhadap overfitting awal, meskipun belum bersifat signifikan.

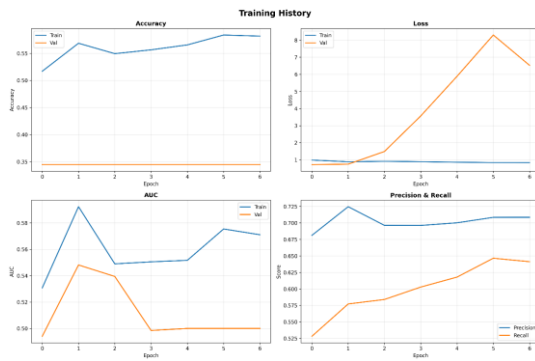
Berdasarkan metrik evaluasi *Precision* dan *Recall*, diperoleh nilai *precision* sebesar 0,70 dan *recall* sebesar 0,625. Nilai *precision* yang relatif lebih tinggi menunjukkan bahwa sebagian besar prediksi *fake* yang dihasilkan oleh model memang benar merupakan video hasil manipulasi. Dengan kata lain, tingkat false

positive yang dihasilkan model relatif rendah, sehingga risiko salah mengklasifikasikan video asli sebagai video manipulasi dapat diminimalkan.

Sebaliknya, nilai *recall* yang lebih rendah mengindikasikan bahwa model belum mampu mendeteksi seluruh video manipulasi yang ada dalam dataset uji. Masih terdapat sejumlah video manipulasi yang diklasifikasikan sebagai video asli (*false negative*). Kondisi ini menunjukkan bahwa meskipun model cukup selektif dan berhati-hati dalam memberikan label *fake*, sensitivitas model terhadap seluruh variasi manipulasi video masih terbatas (Luque et al., 2019; Riehl et al., 2023; Sathyanarayanan, 2024)

Analisis lebih lanjut menunjukkan bahwa kesalahan yang dominan berupa false positive, yaitu kondisi di mana video asli diklasifikasikan sebagai hasil manipulasi. Fenomena ini mengindikasikan bahwa model cenderung sensitif terhadap pola tertentu yang dipelajari dari dataset pelatihan, namun pola tersebut tidak sepenuhnya merepresentasikan karakteristik data pada dataset pengujian yang berbeda. Salah satu faktor utama yang berkontribusi terhadap keterbatasan performa ini adalah keterbatasan sumber daya komputasi, khususnya memori. Meskipun dataset yang tersedia relatif besar, yaitu sekitar 19,8 GB untuk video manipulasi dan 2,7 GB untuk video asli, keterbatasan memori perangkat menyebabkan tidak seluruh dataset dapat digunakan secara optimal dalam proses pelatihan. Akibatnya, model dilatih menggunakan subset data yang lebih kecil, yang berpotensi membatasi cakupan variasi artefak manipulasi yang dapat dipelajari.

Kondisi ini menyebabkan model kurang mampu melakukan generalisasi terhadap dataset dengan karakteristik yang berbeda, sehingga meningkatkan risiko kesalahan klasifikasi, khususnya dalam bentuk false positive. Oleh karena itu, hasil ini menunjukkan bahwa performa model masih sangat dipengaruhi oleh distribusi data pelatihan dan belum sepenuhnya robust terhadap variasi data yang lebih luas



Gambar 4. Confusion Matrics

```
Test Metrics:
Loss: 0.8731
Compile_metrics: 0.5421

Classification Report:
      precision    recall  f1-score   support

 Real (0)       0.4839    0.1210    0.1935     248
 Fake (1)       0.5496    0.8926    0.6803     298

 accuracy              0.5421     546
 macro avg              0.5167     546
 weighted avg           0.5197     546

Confusion Matrix:
True Negatives: 30
False Positives: 218
False Negatives: 32
True Positives: 266

ROC-AUC Score: 0.4945

Additional Metrics:
Accuracy: 0.5421
Precision: 0.5496
Recall: 0.8926
F1-Score: 0.6803
Model saved to: deepfake_detector_advanced.hs
Training history saved to: training_history_advanced.png
```

Gambar 5. Hasil Klasifikasi

Hasil evaluasi pada dataset uji menunjukkan bahwa model cenderung mengklasifikasikan seluruh sampel sebagai kelas REAL. Hal ini ditunjukkan oleh nilai recall sebesar 1.00 pada kelas REAL dan 0.00 pada kelas FAKE. Kondisi ini mengindikasikan adanya bias prediksi yang kuat terhadap satu kelas, yang kemungkinan disebabkan oleh perbedaan distribusi data antara dataset pelatihan dan pengujian (domain shift), serta keterbatasan data pelatihan akibat kendala sumber daya."

Meskipun nilai *ROC-AUC* sebesar 0.5614 menunjukkan bahwa model masih memiliki kemampuan diskriminatif yang lebih baik dibandingkan tebakan acak, namun kemampuan tersebut tidak dapat dimanfaatkan secara efektif pada threshold klasifikasi yang digunakan.

IV. SIMPULAN DAN SARAN

A. Simpulan

Dari hasil pengujian dengan dataset jenis manipulasi *deep fakes* dengan kualitas .mp4

dan intensitas variasi warna terlihat hasil kompresi menggunakan metode ELA menghasilkan tantangan dalam menentukan akurasi deteksi manipulasi. ELA Error Level Analysis membantu menentukan tahap awal *skrining* dalam bidang forensik. Kemudian diintegrasikan dengan model CNN yang telah dikembangkan. Hasil deteksi manipulasi *deep fakes* memperoleh hasil *accuracy* sebesar 54%. Model belum bisa mengidentifikasi video *Real* dan *Fake*.

B. Saran

Trining dengan dataset yang lebih besar untuk mendapatkan *confusion matrix* meningkatkan nilai akurasi sehingga akurat dan handal dalam mendeteksi manipulasi video.

DAFTAR RUJUKAN

- CPatel, H., & M Patel, M. (2015). An Improvement of Forgery Video Detection Technique using Error Level Analysis. *International Journal of Computer Applications*, 111(15), 26–28. <https://doi.org/10.5120/19615-1508>
- Faroek, D. A. (2024). Deteksi Keaslian Citra Menggunakan Metode Error Level Analysis (ELA) dan Principal Component Analysis (PCA). *Acme*, 23(2), 156–160. <https://doi.org/10.7202/1111254ar>
- Harika Palivela, L., Bala Gayathri, D., & Shanmuga Priya, R. (2023). Video Tampering Detection in Real Time. In J. S. Raj, I. Perikos, & V. E. Balas (Eds.), *Intelligent Sustainable Systems* (pp. 351–364). Springer Nature Singapore. https://doi.org/10.1007/978-981-99-1726-6_27
- Idlbeq, R., Pešić, M., & Šolić, K. (2024). Enhancing Digital Image Forensics with Error Level Analysis (ELA). *2024 47th MIPRO ICT and Electronics Convention (MIPRO)*, 1555–1560. <https://doi.org/10.1109/MIPRO60963.2024.10569232>
- Jeronymo, D. C., Borges, Y. C. C., & Coelho, L. dos S. (2017). Image forgery detection by semi-automatic wavelet soft-Thresholding with error level analysis. *Expert Systems with Applications*, 85, 348–356. <https://doi.org/10.1016/j.eswa.2017.05.044>

- Kaur, A., Noori Hoshyar, A., Saikrishna, V., Firmin, S., & Xia, F. (2024). Deepfake video detection: challenges and opportunities. In *Artificial Intelligence Review* (Vol. 57, Issue 6). Springer Netherlands. <https://doi.org/10.1007/s10462-024-10810-6>
- Kaur, H., & Jindal, N. (2020). Image and Video Forensics: A Critical Survey. *Wireless Personal Communications*, 112(2), 1281–1302. <https://doi.org/10.1007/s11277-020-07102-x>
- Mercier, G., Markatopoulou, F., Cozien, R., Zampoglou, M., Apostolidis, E., Metsai, A. I., Papadopoulos, S., Mezaris, V., Patras, I., & Kompatsiaris, I. (2019). Detecting manipulations in video. *Video Verification in the Fake News Era*, 161–189. https://doi.org/10.1007/978-3-030-26752-0_6
- Mohammed, K. B., Agrawal, I., Kandimalla, M. D., Govathoti, P. F., Prakash, C. S., & Singh, P. (2024). Advancing Digital Image Forensics: Enhancing Image Forgery Detection Through Error Level Analysis and Convolutional Neural Networks. In M. Pant, K. Deep, & A. Nagar (Eds.), *Proceedings of the 12th International Conference on Soft Computing for Problem Solving* (pp. 325–340). Springer Nature Singapore.
- Mohiuddin, S., Malakar, S., Kumar, M., & Sarkar, R. (2023). A comprehensive survey on state-of-the-art video forgery detection techniques. *Multimedia Tools and Applications*, 82(22), 33499–33539. <https://doi.org/10.1007/s11042-023-14870-8>
- More, S. S., Lobo, V. B., Chaudhari, A., Pandey, A., Kumavat, B., & Kamble, Y. (2024). Enhancing Image Forgery Detection with Convolutional Neural Networks and Error Level Analysis. In *Journal of Information Systems Engineering and Management* (Vol. 2025, Issue 27s). <https://www.jisem-journal.com/>
- Nagm, A. M., Moussa, M. M., Shoitan, R., Ali, A., Mashhour, M., Salama, A. S., & AbdulWakel, H. I. (2024). Detecting image manipulation with ELA-CNN integration: a powerful framework for authenticity verification. *PeerJ Computer Science*, 10, e2205. <https://doi.org/10.7717/peerj-cs.2205>
- Panchal, H. D., & Shah, H. B. (2020). Video tampering dataset development in temporal domain for video forgery authentication. *Multimedia Tools and Applications*, 79(33–34), 24553–24577. <https://doi.org/10.1007/s11042-020-09205-w>
- Patel, H., & Patel, M. (2015). *Forgery Frame Detection From The Video Using Error Level Analysis*. <https://api.semanticscholar.org/CorpusID:212513110>
- R. Gorle and A. Guttavelli. (2025). *Enhanced Image Tampering Detection using Error Level Analysis and a CNN*. <https://doi.org/https://doi.org/10.48084/etasr.9593>
- Rafique, R., Gantassi, R., Amin, R., Frnda, J., Mustapha, A., & Alshehri, A. H. (2023). Deep fake detection and classification using error-level analysis and deep learning. *Scientific Reports*, 13(1), 1–13. <https://doi.org/10.1038/s41598-023-34629-3>
- Rafique, R., Nawaz, M., Kibriya, H., & Masood, M. (2021). DeepFake Detection Using Error Level Analysis and Deep Learning. *2021 4th International Conference on Computing & Information Sciences (ICCIS)*, 1–4. <https://doi.org/10.1109/ICCIS54243.2021.9676375>
- Raković, D. (2023). Error level analysis (ELA). *Tehnika*, 78(4), 445–451. <https://doi.org/10.5937/tehnika2304445r>
- Sandhya, & Kashyap, A. (2024). A comprehensive analysis of digital video forensics techniques and challenges. *Iran Journal of Computer Science*, 7(2), 359–380. <https://doi.org/10.1007/s42044-023-00165-6>
- Sari, T., Riadi, I., & Fadlil, A. (2016). *Forensik Citra untuk Deteksi Rekayasa File Menggunakan Error Level Analysis*. 2(1), 133–138. <http://ars.ilkom.unsri.ac.id>
- Sari, W. P., & Fahmi, H. (2021). Effect of Error Level Analysis on The Image Forgery Detection Using Deep Learning. *Kinetik:*

- Game Technology, Information System, Computer Network, Computing, Electronics, and Control*, 4(3).
<https://doi.org/10.22219/kinetik.v6i3.1272>
- Vasudevan, M., Sireesha, C., Sumiya, N., Vardhan, K. V., & Sagar, T. (2025). CNN based Error Level Analysis (ELA) With Scores to Detect Digital Image Manipulation. *2025 3rd International Conference on Self Sustainable Artificial Intelligence Systems (ICSSAS)*, 1541–1547.
<https://doi.org/10.1109/ICSSAS66150.2025.11081309>
- Verma, A., Pandey, P., & Khari, M. (2024). ELA-Conv: Forgery Detection in Digital Images Based on ELA and CNN. In K. C. Santosh, A. Makkar, M. Conway, A. K. Singh, A. Vacavant, A. el Kalam, M.-R. Bouguelia, & R. Hegadi (Eds.), *Recent Trends in Image Processing and Pattern Recognition* (pp. 213–226). Springer Nature Switzerland.
- Warif, N. B. A., Idris, Mohd. Y. I., Wahab, A. W. A., & Salleh, R. (2015). An evaluation of Error Level Analysis in image forensics. *2015 5th IEEE International Conference on System Engineering and Technology (ICSET)*, 23–28.
<https://doi.org/10.1109/ICSEngT.2015.7412439>
- Yallamandhala, P., & Godwin, J. (2022). A Review on Video Tampering Analysis and Digital Forensic. In G. Manogaran, A. Shanthini, & G. Vadivu (Eds.), *Proceedings of International Conference on Deep Learning, Computing and Intelligence* (pp. 287–294). Springer Nature Singapore.