

LAPORAN PENELITIAN
PENELITIAN KOLABORASI ANTAR PERGURUAN TINGGI
UIN SUNAN KALIJAGA YOGYAKARTA TAHUN 2022



DETEKSI CITRA WAJAH PALSU GENERATIVE ADVERSARIAL NETWORKS
MENGGUNAKAN CONVOLUTIONAL NEURAL NETWORK BERBASISKAN
ERROR LEVEL ANALYSIS

Tim Peneliti:

Maria Ulfah Siregar (UIN Sunan Kalijaga Yogyakarta)

Nurochman (UIN Sunan Kalijaga Yogyakarta)

Dwi Larasati (UIN Sunan Kalijaga Yogyakarta)

Anif Hanifa Setianingrum (UIN Syarif Hidayatullah)

UNIVERSITAS ISLAM NEGERI
SUNAN KALIJAGA YOGYAKARTA

TAHUN 2022

ABSTRAK

Generative adversarial networks merupakan algoritma yang sering digunakan untuk melakukan generate gambar menggunakan AI. Diperlukan sebuah algoritma yang mampu melakukan deteksi apakah sebuah gambar merupakan hasil kerja generative adversarial networks atau gambar nyata. Pada penelitian ini, kami mengajukan penggunaan algoritma Error Level Analysis dan convolutional neural network untuk mendeteksi citra manipulasi yang dihasilkan oleh generative adversarial networks. Setelah melakukan training data, dapat dibuktikan bahwa penggunaan convolutional neural network dengan kompresi Error Level Analysis dapat meningkatkan performa keseluruhan dari model, baik itu akurasi, precision, recall, maupun parameter lainnya. Berdasarkan hasil evaluasi, didapatkan bahwa training convolutional neural network terbaik didapatkan ketika menggunakan kompresi Error Level Analysis 50% karena dapat mencapai 94% akurasi, precision 93.3%, Recall 94.9%, F1 Score 94.1%, ROC-AUC Score 98.7%, dan AP Score 98.8%. Penelitian ini diharapkan dapat menjadi referensi untuk melakukan proses deteksi gambar antara gambar nyata atau gambar palsu hasil generative adversarial networks.

ABSTRACT

Generative adversarial networks are algorithms that are often used to generate images using AI. An algorithm is needed that is capable of detecting whether an image is the work of generative adversarial networks or a real image. In this study, we propose the use of Error Level Analysis and convolutional neural network algorithms to detect manipulated images generated by generative adversarial networks. After conducting data training, it can be proven that the use of convolutional neural networks with Error Level Analysis compression can improve the overall performance of the model, be it accuracy, precision, recall, or other parameters. Based on the evaluation results, it was found that the best convolutional neural network training was obtained when using 50% Error Level Analysis compression because it can achieve 94% accuracy, 93.3% precision, 94.9% Recall, 94.1% F1 Score, 98.7% ROC-AUC Score, and AP Score 98.8%. This research is expected to be a reference for performing image detection processes between real images or fake images resulting from generative adversarial networks.

نبذة مختصرة

شبكات الخصومة التوليدية هي خوارزميات تُستخدم غالبًا لإنشاء الصور باستخدام الذكاء الاصطناعي. هناك حاجة إلى خوارزمية قادرة على اكتشاف ما إذا كانت الصورة من عمل شبكات الخصومة التوليدية أو صورة حقيقية. في هذه الدراسة نقترح استخدام تحليل مستوى الخطأ وخوارزميات الشبكة العصبية التلافيفية لاكتشاف الصور التي تم التلاعب بها والتي ، تم إنشاؤها بواسطة شبكات الخصومة التوليدية. بعد إجراء التدريب على البيانات ، يمكن إثبات أن استخدام الشبكات العصبية غير المنطقية مع ضغط تحليل مستوى الخطأ يمكن أن يحسن الأداء العام للنموذج ، سواء كان ذلك من حيث الدقة أو الدقة أو الاسترجاع أو معلومات أخرى. بناءً على نتائج التقييم ، وجد أنه تم الحصول على أفضل تدريب على الشبكة العصبية عند استخدام ضغط تحليل مستوى الخطأ بنسبة 50٪ لأنه يمكن أن يحقق دقة 94٪ ، دقة 93.3٪ ، استرجاع 94.9٪ ، 94.1 F1 ، 98.7٪ ROC ، ودرجة AP 98.8٪ مجموع نقاط الجامعة الأمريكية في الولايات المتحدة ، ودرجة - 98.7٪ ROC ، ودرجة F1 ، 94.1 من المتوقع أن يكون هذا البحث مرجعاً لإجراء عمليات الكشف عن الصور بين الصور الحقيقية أو الصور المزيفة الناتجة عن شبكات الخصومة التوليدية.

DAFTAR ISI

BAB I PENDAHULUAN

I. LATAR BELAKANG.....	1
II. RUMUSAN MASALAH.....	1
III. TUJUAN PENELITIAN.....	1
IV. MANFAAT PENELITIAN	1
V. BATASAN PENELITIAN.....	2
VI. RUANG LINGKUP PENELITIAN	2

BAB II KERANGKA TEORI

I. TINJAUAN PUSTAKA.....	3
II. KAJIAN TEORI	3

BAB III METODOLOGI PENELITIAN

Gambar 1. Alur penelitian.....	5
I.1. Pengumpulan Data.....	5
I.2. Pra-pemrosesan Citra.....	6
I.3. Deteksi Tepi dengan Canny Edge Detector	6
I.4. Kompresi Citra dengan ELA	6
I.5. Pendeteksian Citra oleh CNN	6
I.6. Analisis Pendeteksian Citra	6
Tabel 1. Parameter CNN.....	6
Gambar 2. Arsitektur CNN yang dikembangkan.....	8

BAB IV HASIL DAN PEMBAHASAN

I. HASIL DAN PEMBAHASAN	9
Tabel 2. Proses Kompresi ELA pada Wajah Asli dan Wajah Palsu	9
Tabel 3. Proses Kompresi ELA pada Wajah Asli dan Wajah Palsu	10
Tabel 4. Hasil Training dan Validasi Sistem	10
Gambar 3. Akurasi model dari CNN tanpa ELA	11
Gambar 4. Loss model dari CNN tanpa ELA	11
Gambar 5. Akurasi model dari CNN dan ELA 10%.....	11
Gambar 6. Loss model dari CNN dan ELA 10%.....	11
Gambar 7. Akurasi model dari CNN dan ELA 50%.....	11
Gambar 8. Loss model dari CNN dan ELA 50%.....	11
Gambar 9. Akurasi model dari CNN dan ELA 90%.....	12

Gambar 10. Loss model dari CNN dan ELA 90%.....	12
Tabel 5.Evaluasi Kinerja Sistem.....	12

BAB V KESIMPULAN DAN SARAN

DAFTAR BIBLIOGRAFI

BAB I

PENDAHULUAN

I. LATAR BELAKANG

Citra wajah banyak digunakan untuk sistem keamanan, keuangan, pendidikan, keamanan sosial, dan lain-lain (Wu et al., 2020). Di sisi lain, kemajuan teknologi dan ilmu pengetahuan saat ini memudahkan seseorang untuk memanipulasi citra, termasuk citra wajah. Salah satu kemajuan yang dimaksud adalah menciptakan citra palsu yang sangat mendekati citra asli dengan menggunakan generative adversarial network (GAN). Beberapa penelitian sebelumnya telah mengusulkan metode untuk mendeteksi citra palsu yang dihasilkan oleh GAN (Neves et al., 2020)(Venkatesh et al., 2020). Pada penelitian ini, kami mengajukan penggunaan algoritma error level analysis (ELA) dan convolutional neural network (CNN) untuk mendeteksi citra manipulasi yang dihasilkan oleh GAN.

II. RUMUSAN MASALAH

Berdasarkan latar belakang di atas, rumusan masalah adalah bagaimana menerapkan algoritma ELA sebagai pra-pemrosesan pada CNN untuk mendeteksi keaslian citra wajah yang dihasilkan oleh GAN. Selanjutnya, bagaimana keakuratan pendeteksian yang kami ajukan, dan apakah pengimplementasian ELA sebelum proses di CNN bisa meningkatkan keakuratan pendeteksian.

III. TUJUAN PENELITIAN

Penelitian ini bertujuan menerapkan ELA sebagai pra-pemrosesan pada CNN dan menganalisis keakuratan penerapan tersebut dalam mendeteksi apakah suatu citra wajah adalah asli atau hasil manipulasi oleh GAN.

IV. MANFAAT PENELITIAN

Manfaat dari penelitian ini adalah memberikan alternatif penerapan ELA sebagai pra-pemrosesan pada CNN. Selain itu, penelitian ini juga memberikan analisis keakuratan penerapan tersebut dalam mendeteksi apakah suatu citra wajah adalah asli atau hasil manipulasi oleh GAN.

V. BATASAN PENELITIAN

Batasan yang ditetapkan pada penelitian ini adalah dataset yang digunakan adalah dataset publik dari Kaggle. Batasan lainnya adalah level kompresi ELA hanya tiga yaitu: 10%, 50%, dan 90%. Selanjutnya, untuk algoritma kompresi ELA, dan Canny Edge Detector, diambil dari library Python.

VI. RUANG LINGKUP PENELITIAN

Penelitian ini mengusulkan penerapan ELA pada CNN dan menganalisis keakuratannya. Sehingga kami tidak meneliti mengenai algoritma ELA secara mendalam. Demikian juga dengan algoritma deteksi tepi Canny Edge Detector tidak diteliti secara mendalam di dalam penelitian ini.

BAB II

KERANGKA TEORI

I. TINJAUAN PUSTAKA

Metode GANprintR ditujukan untuk mendeteksi citra wajah manipulasi yang dihasilkan oleh GAN (Neves et al., 2020). Teknik yang dilakukan adalah dengan menghilangkan GAN *fingerprints* dari citra palsu. Hasil penelitian tersebut adalah masih diperlukan usaha tambahan untuk mengembangkan sistem deteksi citra manipulasi yang tangguh. Penelitian lainnya melakukan enkripsi pada fitur wajah yang berdasarkan pada GAN (Wu et al., 2020). Enkripsi yang merupakan proses satu arah yang tidak bisa dibalik, melindungi fitur wajah dengan baik. Permasalahan citra yang tidak jelas (*blur*) coba diselesaikan di dalam suatu penelitian. Citra wajah dan tubuh yang *blur* direstorasi dengan menggunakan GAN (Koo et al., 2020).

Penelitian yang menggabungkan ELA dan deep learning (DL) sudah pernah dilakukan oleh peneliti lain. Salah satunya penelitian yang berjudul "Deteksi Pemalsuan Gambar dengan ELA dan Deep Learning" (Gunawan et al., 2018). Pada penelitian tersebut digunakan 1771 gambar dengan label *tampered* dan 2940 gambar dengan label *real* yang diambil dari CASIA dataset.

II. KAJIAN TEORI

GANs adalah suatu *framework* baru yang digunakan untuk mengestimasi model-model generatif melalui suatu proses *adversarial* (Goodfellow et al., 2014). Pada *framework* tersebut, secara bersamaan dua model ditraining: satu model generatif G yang mewakili distribusi data, dan satu model diskriminatif D yang mengestimasi probabilitas bahwa satu sampel berasal dari data training selain G . Prosedur training bagi G adalah untuk memaksimalkan probabilitas dari G berbuat suatu kesalahan.

GAN sudah diintegrasikan dengan CNNs dan menghasilkan satu kelas CNN yaitu deep convolutional generative adversarial network (DCGANs). Kelas ini memiliki batasan arsitektur dan diklaim sebagai kandidat yang tangguh dari *unsupervised learning* (Radford & Metz, 2016).

CNN awalnya digagas untuk mengenali tulisan tangan, yang kemudian berhasil menyelesaikan permasalahan pengenalan citra, deteksi dan segmentasi citra (Sudiatmika et al., 2019). CNN memiliki kemampuan yang bagus dalam mengklasifikasi citra skala besar. Kemampuan ini dipengaruhi oleh susunan dari suatu CNN yang terdiri dari tiga lapis: lapis convolutional, lapis pooling, dan lapis fully connections.

Canny Edge Detector adalah operator pendeteksi tepi yang menggunakan sebuah algoritma yang terdiri dari beberapa tahap untuk mendeteksi banyak tepi di dalam citra. Operator ini dikembangkan oleh John F. Canny di tahun 1986 (Sofiane Sahir, 2019). Langkah-langkah di dalam algoritma pendeteksi ini adalah:

1. Noise reduction
2. Gradient calculation
3. Non-maximum suppression
4. Double threshold
5. Edge Tracking by Hysteresis

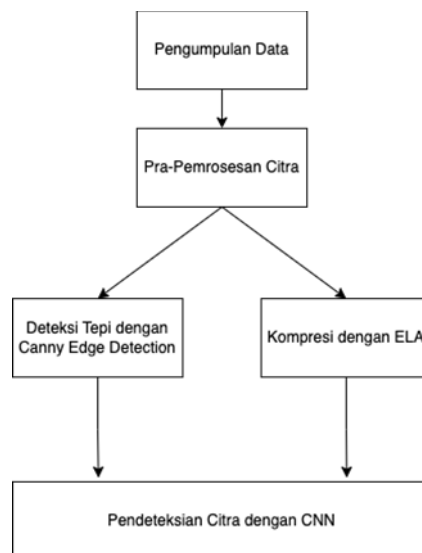
Algoritma di atas diterapkan pada gambar keabuan (grayscale). Sehingga, adalah suatu kebutuhan untuk mengkonversi citra menjadi keabuan sebelum langkah-langkah di atas dapat diterapkan.

ELA adalah suatu metode forensik dalam mengidentifikasi bagian-bagian dari suatu citra berdasarkan pada perbedaan tingkat kompresinya (Faroek et al., 2020). Suatu citra akan dibagi menjadi 8x8 blok citra kecil dan dikompres menggunakan JPEG sampai keakuratan 95%. Masing-masing blok akan memberikan tingkat kualitas kompresi yang sama, jika ada blok yang berbeda kualitasnya, maka ini mengindikasikan adanya manipulasi (Azhan et al., 2022). Proses ELA bisa dilakukan dengan cara: menyimpan citra menggunakan level kualitas kompresi tertentu, menghitung dan mengamati perbedaan antara level kompresi.

BAB III

METODOLOGI PENELITIAN

Penelitian ini dimulai dengan pengumpulan data citra dari dataset publik, bersamaan dengan dilakukannya studi pustaka. Selanjutnya adalah melakukan pra-pemrosesan citra, kompresi citra dengan ELA, deteksi oleh CNN, dan analisis keakuratan. Pendeteksian citra asli dan palsu menggunakan dua skenario: yang diawali dengan kompresi citra dengan ELA, dan yang tidak diawali dengan kompresi citra ELA. Untuk skenario yang pertama ada tiga subskenario yaitu dengan level kompresi 10%, 50%, dan 90%. Sedangkan untuk skenario kedua, dilakukan pra-pemrosesan dengan Canny Edge Detector. Gambar 1 menunjukkan alur penelitian yang kami lakukan.



Gambar 1. Alur penelitian

I.1. Pengumpulan Data

Pada penelitian ini digunakan dataset publik dari Kaggle yaitu 140k Real and Fake Faces (xhlulu, n.d.). Dataset terdiri dari 70 ribu wajah asli, dan 70 ribu wajah palsu yang dihasilkan dari StyleGAN. Citra berukuran 256 piksel dan dibagikan ke dalam tiga folder: train, validation, dan test. Dataset train berisikan 100 ribu wajah yang dibagi dua sehingga citra wajah asli sejumlah 50 ribu, dan citra wajah palsu sejumlah 50 ribu. Dataset validation berisikan 20 ribu wajah dengan citra wajah asli sejumlah 10 ribu dan citra wajah palsu sejumlah 10 ribu. Dataset testing dengan penjelasan yang sama dengan dataset validation.

I.2. Pra-pemrosesan Citra

Ukuran citra dari dataset yang cukup besar akan menyulitkan saat running sistem di Google Colab. Pilihan running secara online ini adalah disediakannya GPU yang bisa mempercepat proses running. Sehingga pada tahapan pra-pemrosesan citra, ukuran citra diperkecil menjadi 150 piksel. Untuk skenario deteksi tanpa ELA, pra-pemrosesan citra dilanjutkan dengan mengaplikasikan Canny Edge Detector.

I.3. Deteksi Tepi dengan Canny Edge Detector

Proses deteksi tepi ini dilakukan untuk skenario tanpa ELA. Dengan diterapkannya algoritma deteksi tepi ini, pendeteksian citra menjadi lebih akurat.

I.4. Kompresi Citra dengan ELA

Pada penelitian ini kami menggunakan tiga level kompresi citra pada ELA yaitu 10%, 50%, dan 90%. Pilihan level kompresi tersebut adalah berdasarkan pada penelitian-penelitian sebelumnya. Dari hasil kompresi ini dihasilkan citra yang sudah terbagi ke dalam citra-citra kecil yang sudah dikompresi dengan JPEG sesuai dengan level kompresinya.

I.5. Pendeteksian Citra oleh CNN

Tabel 1 memberikan informasi mengenai parameter CNN yang digunakan di dalam penelitian ini. Sedangkan Gambar 2 menunjukkan arsitektur CNN yang digunakan di dalam penelitian.

I.6. Analisis Pendeteksian Citra

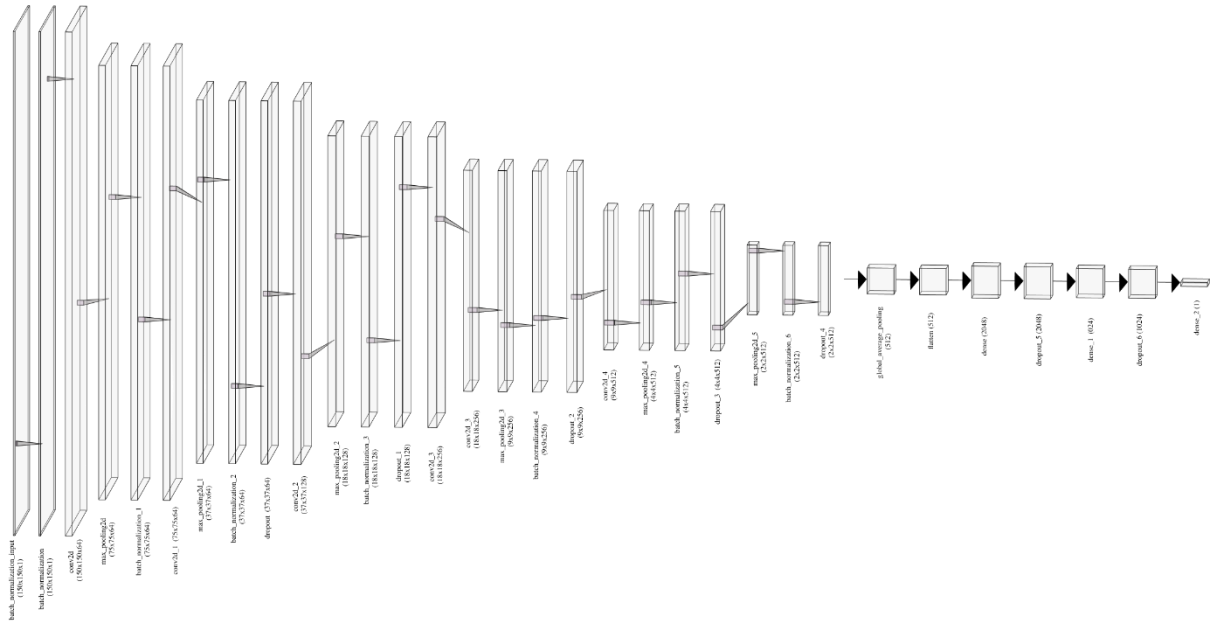
Untuk menganalisis hasil pendeteksian citra, kami menggunakan analisis keakuratan pendeteksian. Analisis tersebut didasarkan pada metode yang diberikan di Python. Untuk menganalisis proses training dan validasi, kami gunakan nilai akurasi (accuracy), nilai loss, dan waktu yang digunakan untuk proses. Sedangkan untuk proses testing, kami menganalisis nilai akurasi (accuracy), nilai presisi (precision), nilai recall, nilai F1, nilai ROC-AUC, dan nilai AP.

Tabel 1. Parameter CNN

Layer	Volume	Parameter
-------	--------	-----------

batch_normalization_input (InputLayer)	150x150x1	0
batch_normalization (BatchNormalization)	150x150x1	4
conv2d (Conv2D)	150x150x64	640
max_pooling2d (MaxPooling2D)	75x75x64	0
batch_normalization_1 (BatchNormalization)	75x75x64	256
conv2d_1 (Conv2D)	75x75x64	36928
max_pooling2d_1 (MaxPooling2D)	37x37x64	0
batch_normalization_2 (BatchNormalization)	37x37x64	256
dropout (Dropout)	37x37x64	0
conv2d_2 (Conv2D)	37x37x128	73856
max_pooling2d_2 (MaxPooling2D)	18x18x128	0
batch_normalization_3 (BatchNormalization)	18x18x128	512
dropout_1 (Dropout)	18x18x128	0
conv2d_3 (Conv2D)	18x18x256	295168
max_pooling2d_3 (MaxPooling2D)	9x9x256	0
batch_normalization_4 (BatchNormalization)	9x9x256	1024
dropout_2 (Dropout)	9x9x256	0
conv2d_4 (Conv2D)	9x9x512	1180160
max_pooling2d_4 (MaxPooling2D)	4x4x512	0
batch_normalization_5 (BatchNormalization)	4x4x512	2048
dropout_3 (Dropout)	4x4x512	0
conv2d_5 (Conv2D)	4x4x512	2359808
max_pooling2d_5 (MaxPooling2D)	2x2x512	0
batch_normalization_6 (BatchNormalization)	2x2x512	2048
dropout_4 (Dropout)	2x2x512	0
global_average_pooling (GlobalAveragePooling2D)	512	0
flatten (Flatten)	512	0
dense (Dense)	2048	1050624
dropout_5 (Dropout)	2048	0
dense_1 (Dense)	1024	2098176

dropout_6 (Dropout)	1024	0
dense_2 (Dense)	1	1025
Total params: 7,102,533		
Trainable params: 7,099,459		
Non-trainable params : 3,074		



Gambar 2. Arsitektur CNN yang dikembangkan

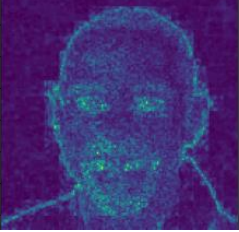
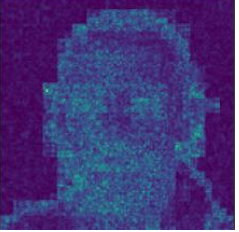
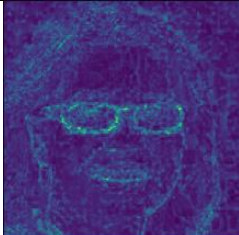
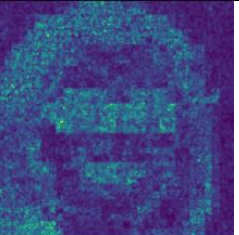
BAB IV

HASIL DAN PEMBAHASAN

I. HASIL DAN PEMBAHASAN

Tabel 2 menunjukkan proses kompresi ELA pada satu citra wajah asli dan satu citra wajah palsu. Kompresi ELA terdiri dari tiga level kompresi, yaitu 10%, 50%, dan 90%. Jika diperhatikan, citra wajah asli memberikan kualitas warna yang sama di setiap level kompresi ELA. Sedangkan pada citra wajah palsu, ada bagian-bagian wajah yang memiliki kualitas warna yang berbeda pada setiap level kompresinya.

Tabel 2. Proses Kompresi ELA pada Wajah Asli dan Wajah Palsu

	ELA 10%	ELA 50%	ELA 90%
Real Image			
Image			
With ELA Compression			
Fake Image			
Image			
With ELA Compression			

Tabel 3 menunjukkan proses deteksi tepi dengan algoritma Edge Canny Detection. Dengan diterapkannya algoritma pendeteksi tepi tersebut, proses deteksi citra wajah menjadi lebih akurat.

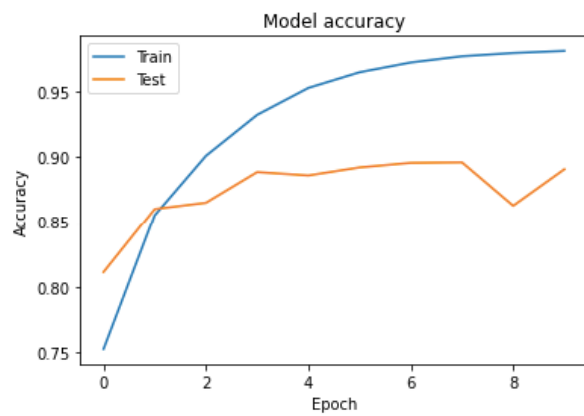
Tabel 3. Proses Kompresi ELA pada Wajah Asli dan Wajah Palsu

	Real Image	Fake Image
Original Image		
With Canny Edge Detection		

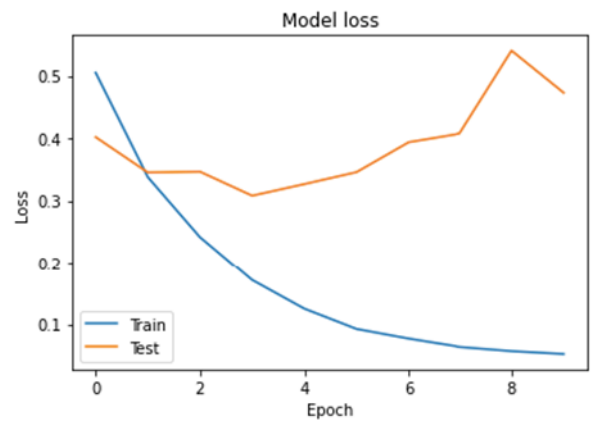
Tabel 4 menunjukkan hasil training dan validasi sistem yang berdasarkan pada akurasi, loss, dan waktu. Gambar 3-10 menunjukkan akurasi model dan loss model untuk empat skenario penelitian yang ditunjukkan pada Tabel 4. Tabel 5 menunjukkan hal yang sama tetapi dari testing/pengujian sistem.

Tabel 4. Hasil Training dan Validasi Sistem

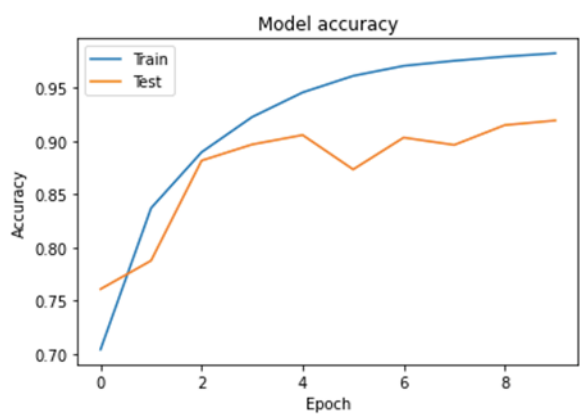
	Tanpa ELA	ELA 10%	ELA 50%	ELA 90%
Accuracy	0.9806	0.9827	0.9860	0.9830
Loss	0.0525	0.0475	0.0386	0.0479
Validation Accuracy	0.8906	0.9196	0.9374	0.9129
Validation Loss	0.4729	0.2907	0.2236	0.3389
Test Accuracy	0.89155	0.92305	0.94085	0.9161
Time (s)	102	102	102	103



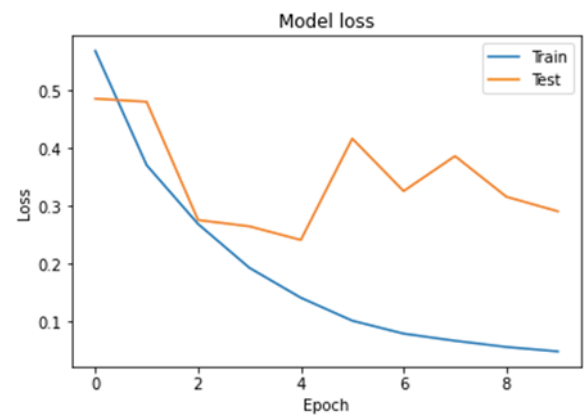
Gambar 3. Akurasi model dari CNN tanpa ELA



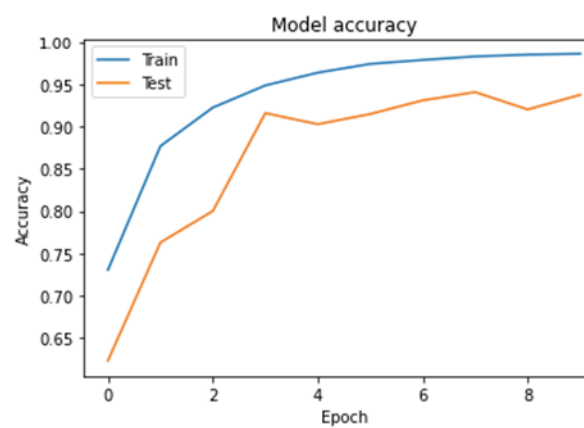
Gambar 4. Loss model dari CNN tanpa ELA



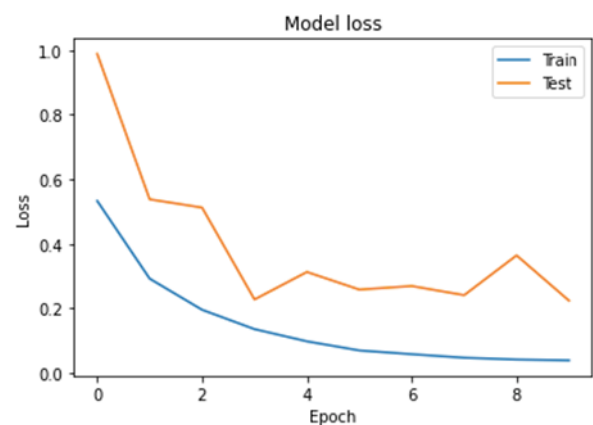
Gambar 5. Akurasi model dari CNN dan ELA 10%



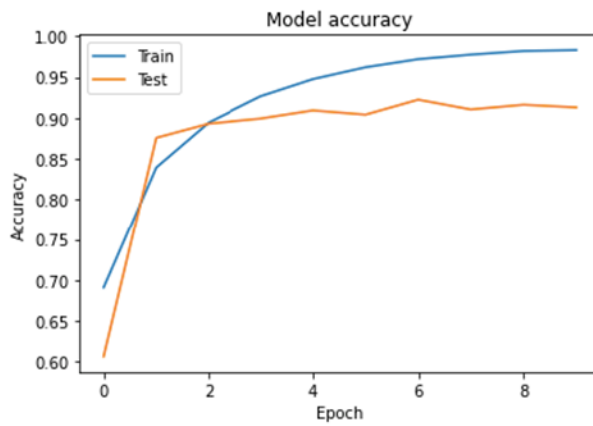
Gambar 6. Loss model dari CNN dan ELA 10%



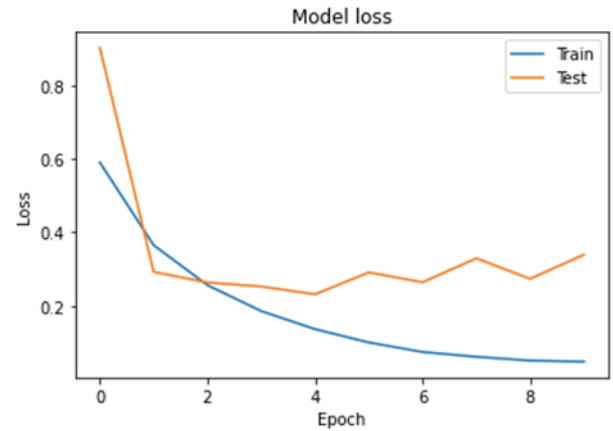
Gambar 7. Akurasi model dari CNN dan ELA 50%



Gambar 8. Loss model dari CNN dan ELA 50%



Gambar 9. Akurasi model dari CNN dan ELA 90%



Gambar 10. Loss model dari CNN dan ELA 90%

Tabel 5. Evaluasi Kinerja Sistem

	Tanpa ELA	ELA 10%	ELA 50%	ELA 90%
Accuracy Score	0.89155	0.92305	0.94085	0.9161
Precision Score	0.86245	0.929885	0.93369	0.92407
Recall Score	0.9317	0.9151	0.9491	0.9067
F1 Score	0.89574	0.92243	0.94133	0.91530
ROC AUC Score	0.96333	0.97683	0.98733	0.97349
AP Score	0.96671	0.97826	0.98813	0.97571

Berdasarkan Tabel 4 di atas, hasil akurasi dalam proses learning sistem pendeteksi yang dikembangkan adalah sangat baik. Demikian juga hasil validasi terhadap proses training adalah baik. Akurasi paling besar dan loss paling sedikit diperoleh saat ELA dengan level kompresi 50% diterapkan sebelum pendeteksian dengan CNN dilakukan. Kebalikannya adalah tanpa ELA, yang menunjukkan hasil paling rendah di antara empat skenario yang telah dilakukan.

Selanjutnya Tabel 5 menunjukkan evaluasi kinerja sistem. Berdasarkan Tabel 4, proses pendeteksian citra asli dan palsu adalah lebih baik kinerjanya jika proses CNN didahului dengan kompresi ELA, khususnya 50%. Berdasarkan evaluasi model, dibuktikan bahwa penggunaan ELA dapat meningkatkan performa keseluruhan dari model yang didesain. Performa tertinggi dimiliki oleh training CNN ELA 50% sebesar 94% Accuracy, Precision 93.3%, Recall 94.9%, F1 Score 94.1%, ROC-AUC Score 98.7%, dan AP Score 98.8%.

BAB V

KESIMPULAN DAN SARAN

Untuk mendeteksi apakah sebuah citra merupakan hasil kerja GAN (citra palsu) atau citra sebenarnya, dapat digunakan algoritma CNN dengan metode kompresi ELA. Setelah melakukan training data dapat dibuktikan bahwa penggunaan CNN dengan kompresi ELA dapat meningkatkan performa keseluruhan dari model, baik itu akurasi, precision, recall, maupun parameter lainnya. Berdasarkan hasil evaluasi, didapatkan bahwa training CNN terbaik didapatkan ketika menggunakan kompresi ELA 50% karena dapat mencapai 94.1% akurasi. Penelitian ini diharapkan dapat menjadi referensi untuk melakukan proses deteksi citra antara citra asli atau citra palsu hasil GAN.

Untuk penelitian selanjutnya, bisa menggunakan lebih dari satu metode learning sehingga bisa dibandingkan performa yang lebih baik. Selain itu, level kompresi ELA bisa divariasikan.

DAFTAR BIBLIOGRAFI

- Azhan, N. A. N., Ikuesan, R. A., Razak, S. A., & Kebande, V. R. (2022). Error Level Analysis Technique for Identifying JPEG Block Unique Signature for Digital Forensic Analysis. *Electronics (Switzerland)*, 11(9). <https://doi.org/10.3390/electronics11091468>
- Farook, D. A., Umar, R., & Riadi, I. (2020). Deteksi Keaslian Citra Menggunakan Metode Error Level Analysis (ELA) dan Principal Component Analysis (PCA). *Format : Jurnal Ilmiah Teknik Informatika*, 8(2), 132. <https://doi.org/10.22441/format.2019.v8.i2.006>
- Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., Courville, A., & Bengio, Y. (2014). Generative Adversarial Nets. *Neural Information Processing Systems* 27. <https://papers.nips.cc/paper/2014/file/5ca3e9b122f61f8f06494c97b1afccf3-Paper.pdf>
- Gunawan, A., Lovenia, H., & Pramudita, A. H. (2018). *DETEKSI PEMALSUAN GAMBAR DENGAN ELA DAN DEEP LEARNING*. <https://doi.org/http://dx.doi.org/10.13140/RG.2.2.28571.52006>
- Koo, J. H., Cho, S. W., Baek, N. R., & Park, K. R. (2020). Face and Body-Based Human Recognition by GAN-Based Blur Restoration. *Sensors*, 20. chrome-extension://dagcmkpagjlhakfdhnbomgmjdpkdklff/enhanced-reader.html?openApp&pdf=https%3A%2F%2Fmdpi-res.com%2Fd_attachment%2Fsensors%2Fsensors-20-05229%2Farticle_deploy%2Fsensors-20-05229.pdf
- Neves, J. C., Tolosana, R., Vera-Rodriguez, R., Lopes, V., Proença, H., & Fierrez, J. (2020). GANprintR: Improved Fakes and Evaluation of the State of the Art in Face Manipulation Detection. *IEEE Journal on Selected Topics in Signal Processing*, 14(5), 1038–1048. <https://doi.org/10.1109/JSTSP.2020.3007250>
- Radford, A., & Metz, L. (2016). Unsupervised Representation Learning With Deep Convolutional Generative Adversarial Networks. *ICLR*.
- Sofiane Sahir. (2019, January 25). *Canny Edge Detection Step by Step in Python* — *Computer Vision*. Towards Data Science. <https://towardsdatascience.com/canny-edge-detection-step-by-step-in-python-computer-vision-b49c3a2d8123>

Sudiatmika, I. B. K., Rahman, F., Trisno, & Suyoto. (2019). Image forgery detection using error level analysis and deep learning. *Telkomnika (Telecommunication Computing Electronics and Control)*, 17(2), 653–659.

<https://doi.org/10.12928/TELKOMNIKA.V17I2.8976>

Venkatesh, S., Zhang, H., Ramachandra, R., Raja, K., Damer, N., & Busch, C. (2020). Can GAN Generated Morphs Threaten Face Recognition Systems Equally as Landmark Based Morphs? - Vulnerability and Detection. *IWBF 2020*.

[https://www.researchgate.net/profile/Haoyu-Zhang-](https://www.researchgate.net/profile/Haoyu-Zhang-24/publication/340666544_Can_GAN_Generated_Morphs_Threaten_Face_Recognition_Systems_Equally_as_Landmark_Based_Morphs_-_Vulnerability_and_Detection/links/5ea469b2299bf112560e6482/Can-GAN-Generated-Morphs-Thre)

[24/publication/340666544_Can_GAN_Generated_Morphs_Threaten_Face_Recognition_Systems_Equally_as_Landmark_Based_Morphs_-](https://www.researchgate.net/profile/Haoyu-Zhang-24/publication/340666544_Can_GAN_Generated_Morphs_Threaten_Face_Recognition_Systems_Equally_as_Landmark_Based_Morphs_-_Vulnerability_and_Detection/links/5ea469b2299bf112560e6482/Can-GAN-Generated-Morphs-Thre)

[Vulnerability_and_Detection/links/5ea469b2299bf112560e6482/Can-GAN-Generated-Morphs-Thre](https://www.researchgate.net/profile/Haoyu-Zhang-24/publication/340666544_Can_GAN_Generated_Morphs_Threaten_Face_Recognition_Systems_Equally_as_Landmark_Based_Morphs_-_Vulnerability_and_Detection/links/5ea469b2299bf112560e6482/Can-GAN-Generated-Morphs-Thre)

Wu, C., Ju, B., Wu, Y., Xiong, N. N., & Zhang, S. (2020). WGAN-E: A generative adversarial networks for facial feature security. *Electronics (Switzerland)*, 9(3).

<https://doi.org/10.3390/electronics9030486>

xhlulu. (n.d.). *140k Real and Fake Faces*.