Scan
Jurnal Teknologi Informasi dan Komunikasi

ISSN (Print): 1978-0087
ISSN (Online): 2686-6099
Volume 19 Nomor 3, Oktober 2024
Halaman: 156-162

Deteksi Gambar Palsu Menggunakan *Deep Learning*

Alif Wildan Azzahra*, Satria Farras Ayhallansyah, Moh. Angga Ardiansyah,
Moh. Ayyuhan Fawwazansa, Fetty Tri Anggraeny
Fakultas Ilmu Komputer,
Universitas Pembangunan Nasional ”Veteran” Jawa Timur, Indonesia

Diterima: Juli, 2024 | Revisi: September, 2024 | Diterbitkan: Oktober 2024

DOI: https://doi.org/10.33005/scan.v19i3.5032

ABTSRAK

Di era digital ini, gambar palsu semakin mudah dibuat dengan teknologi canggih, sehingga penting untuk memiliki cara mendeteksi gambar palsu yang efektif. Penelitian ini menggunakan metode gabungan antara Noiseprint, ResNet-50, dan Support Vector Machine (SVM). Noiseprint membantu menemukan pola noise unik dalam gambar, ResNet-50 menangkap detail fitur gambar yang kompleks, dan SVM memutuskan apakah gambar itu asli atau palsu. Dengan dataset dari Columbia University, metode ini berhasil mencapai akurasi hingga 90,41%. Hasilnya menunjukkan bahwa pendekatan ini sangat menjanjikan untuk mendeteksi gambar palsu jenis splicing. Meski begitu, penelitian ini masih menghadapi keterbatasan, seperti kebutuhan komputasi tinggi dan terbatasnya variasi dataset.

Kata Kunci: *ResNet-50, SVM*, Ekstraksi Fitur, Gambar bertumpuk, *CUISIDE*

Fake Image Detection Using Deep Learning

ABSTRACT

In this digital era, fake images are increasingly easy to create with advanced technology, making it crucial to have effective methods for detecting fake images. This research utilizes a combined approach involving Noiseprint, ResNet-50, and Support Vector Machine (SVM). Noiseprint helps identify unique noise patterns in images, ResNet-50 captures complex image feature details, and SVM determines whether an image is authentic or fake. Using a dataset from Columbia University, this method achieved an accuracy of up to 90.41%. The results indicate that this approach is highly promising for detecting splicing-type fake images. However, the study still faces limitations, such as high computational requirements and limited dataset variety.

Keywords: ResNet-50, SVM, Feature Extraction, Stacked Images, CUISIDE.

***Corresponding Author:**
Email : 21081010312@student.upnjatim.ac.id
Alamat : Jl. Rungkut Madya, Gn. Anyar, Kec. Gn. Anyar, Surabaya, Jawa Timur 60294

PENDAHULUAN

Dalam era digital yang semakin maju, perkembangan perangkat lunak manipulasi gambar telah mengalami kemajuan yang signifikan. Teknologi ini tidak hanya memudahkan pengguna untuk mengedit dan memanipulasi gambar dengan hasil yang sangat realistis, tetapi juga telah membuka peluang bagi penggunaan yang kurang etis. Gambar palsu (*forged images*) yang dihasilkan dengan menggunakan perangkat lunak canggih kini dapat digunakan untuk berbagai tujuan yang merugikan [1]. Dampaknya dapat dirasakan di berbagai sektor, mulai dari penyebaran berita palsu (*fake news*), manipulasi politik, hingga penipuan yang melibatkan lembaga keuangan dan bisnisaf dalam atau *Deep learning* yang terkenal untuk belajar dari data besar dan menangani masalah pelatihan jaringan yang sangat dalam. Arsitektur ini terdiri dari lapisan konvolusi yang terdiri dari 50 lapisan dan *kernel* berukuran 3x3, Residual Blok menggunakan *shortcut connection* untuk mengatasi masalah *vanishing gradient*, fungsi aktivasi *ReLU*, Lapisan *Pooling*, Lapisan *Fully Connected*, dan terakhir adalah lapisan *output* berupa vektor fitur map. Akibatnya, ancaman terhadap kebenaran informasi visual menjadi semakin besar, dan kebutuhan untuk mengembangkan metode yang lebih andal dalam mendeteksi gambar palsu menjadi semakin mendesak.

Pengolahan citra merupakan bagian penting yang mendasari berbagai aplikasi nyata, seperti pengenalan pola, dan pengindraan jarak-jauh melalui satelit atau pesawat udara [2]. Secara tradisional, deteksi gambar palsu dilakukan melalui metode analisis forensik berbasis fitur, yang berfokus pada pencarian anomali atau jejak-jejak manipulasi pada gambar. Teknik-teknik ini melibatkan analisis pola kompresi JPEG, pengidentifikasian *metadata* gambar yang tidak sesuai, serta tidak seragamnya pola pencahayaan pada gambar. Misalnya, ketika sebuah gambar dimanipulasi dan disimpan ulang dalam format JPEG, sering kali terdapat tidak konsistennya pola kompresi yang dapat menunjukkan adanya perubahan. Demikian pula, *metadata* gambar seperti tanggal pengambilan gambar atau pengaturan kamera dapat memberikan petunjuk tentang apakah gambar tersebut telah dimodifikasi. Selain itu, manipulasi gambar yang melibatkan penggabungan elemen-elemen dari berbagai gambar sering kali meninggalkan jejak berupa pencahayaan yang tidak konsisten, yang dapat diidentifikasi sebagai anomali.

Kemunculan *deep learning* telah terbukti sangat kuat dalam mengungkap fitur-fitur tersembunyi yang kompleks dalam data [3]. Dengan kemampuannya untuk menangkap pola dan hubungan yang sulit dikenali oleh metode tradisional, pendekatan ini sering kali menunjukkan kinerja yang sangat baik. Hal ini membuat *deep learning* menjadi salah satu teknologi utama dalam berbagai bidang, seperti pengenalan gambar, pemrosesan bahasa alami, dan analisis data lainnya.

METODE PENELITIAN

Penelitian ini terdiri dari beberapa tahapan. Tahapan-tahapan tersebut akan ditampilkan dalam kerangka gambar 1. Di era digital saat ini, manipulasi gambar telah menjadi hal yang umum, terutama dengan kemudahan akses terhadap perangkat lunak pengeditan gambar yang canggih. Salah satu bentuk manipulasi yang sering terjadi adalah pemalsuan gambar, di mana gambar asli diubah atau digabungkan dengan gambar lain untuk menciptakan kesan yang menyesatkan [4]. Pemalsuan gambar ini tidak hanya terjadi di media sosial, tetapi juga dalam konteks berita dan hukum, di mana keaslian

gambar dapat mempengaruhi opini publik dan keputusan hukum [5]. Oleh karena itu, penting untuk mengembangkan metode yang efektif untuk mendeteksi gambar palsu guna memulihkan kepercayaan publik terhadap informasi visual.

Studi Literatur

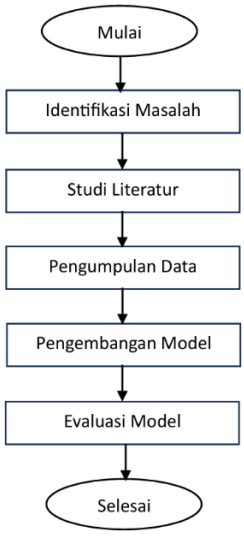
Penelitian tentang deteksi gambar palsu telah berkembang pesat dalam beberapa tahun terakhir, dengan pendekatan yang beragam mulai dari teknik berbasis fitur hingga metode pembelajaran mendalam *(deep learning)*. Metode berbasis fitur tradisional sering kali mengandalkan pengolahan citra untuk mengekstrak karakteristik tertentu dari gambar, seperti pola *noise* atau tekstur [6]. Namun, metode ini memiliki keterbatasan dalam hal akurasi dan ketahanan terhadap teknik pemrosesan gambar lebih lanjut [7].

Dengan munculnya pembelajaran mendalam, banyak peneliti mulai beralih ke model berbasis jaringan saraf konvolusional *(CNN)* yang mampu belajar dari data dalam jumlah besar dan mengekstrak fitur yang lebih kompleks [8]. Penelitian oleh Chen et al. (2019) menunjukkan bahwa penggunaan *CNN* dalam deteksi gambar palsu dapat meningkatkan akurasi secara signifikan dibandingkan dengan metode tradisional [9]. Selain itu, penelitian oleh Hussain et al. (2021) mengusulkan pendekatan baru yang menggabungkan teknik *transfer learning* dan CNN untuk meningkatkan deteksi gambar yang telah dimanipulasi[10].

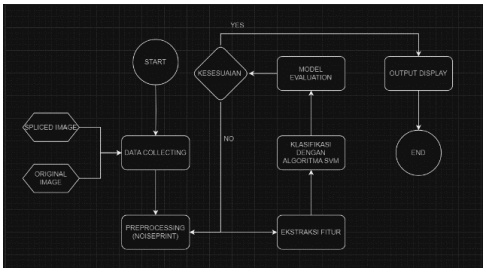
Dengan mempertimbangkan kemajuan ini, penelitian ini bertujuan untuk mengeksplorasi lebih lanjut penggunaan teknik pembelajaran mendalam dalam deteksi gambar palsu, dengan fokus pada pengembangan model yang dapat mengidentifikasi gambar yang telah dimanipulasi secara efektif.

Pengumpulan Data

Proses pengumpulan data dilakukan dengan mengambil data publik bernama *The Columbia Uncompressed Image Splicing Detection Evaluation (CUISDE) dataset*. Data ini diperoleh dari website *columbia University*. Data ini terdiri dari 2 data utama, yakni data gambar yang ditumpuk dan data gambar normal.



Gambar 1. Tahapan Penelitian



Gambar 2. Model yang digunakan dalam penelitian ini.

Pengembangan Model

Model yang digunakan dalam penelitian ini seperti pada gambar 2 terdiri dari 3 struktur utama, yakni *Noiseprint*, *ResNet-50*, dan *Support Vector Machine*. Berikut penjelasan dari masing-masing Model tersebut.

a. *Noiseprint*
   Noiseprint adalah teknik yang digunakan untuk mendeteksi dan mengurangi *noise* yang ada dalam gambar dan dapat dikenali. *Noiseprint* bekerja dengan memahami dan menganalisis pola *noise* yang ada dalam sebuah citra. Cara kerja dari teknik adalah dengan mengolah gambar menggunakan Filter-filter yang telah ditentukan, seperti *High-pass* filter berupa *Gaussian Blur* untuk menyoroti komponen hasil blur, dan median filter untuk mengurangi *noise* dan memperhalus gambar. *Output* dari teknik ini sendiri adalah sebuah peta kebisingan berupa representasi *noise* dari sebuah gambar.

b. ResNet-50
   ResNet-50 adalah sebuah arsitektur jaringan saraf dalam atau *Deep learning* yang terkenal untuk belajar dari data besar dan menangani masalah pelatihan jaringan yang sangat dalam. Arsitektur ini terdiri dari lapisan konvolusi yang terdiri dari 50 lapisan dan *kernel* berukuran 3x3, *Residual Blok* menggunakan *shortcut connection* untuk mengatasi masalah *vanishing gradient,* fungsi aktivasi *ReLU*, Lapisan *Pooling*, Lapisan *Fully Connected*, dan terakhir adalah lapisan *output* berupa vektor fitur *map*.

c. *Support Vector Machine (SVM)*
   SVM adalah algoritma klasifikasi yang banyak digunakan untuk *dataset* dengan dimensi yang tinggi. *SVM* bekerja dengan mencari *hyperplane* optimal yang memisahkan kelas-kelas dalam ruang fitur. Dalam penelitian ini, *SVM* bekerja dengan menerima *input* berupa peta fitur dari *ResNet-50*, kemudian mencari *Hyperplane* untuk memisahkan kelas, *Support Vector* untuk mencari data *poin* yang paling dekat dengan hyperplane, dan hasil *output* berupa hasil prediksi klasifikasi.

Evaluasi

Metode evaluasi yang digunakan menggunakan *Classification report* dengan menampilkan metrik-metrik seperti akurasi, presisi*, recall, F1-score.* Selain itu, peneliti juga menggunakan *Confusion Matrix.*

HASIL DAN PEMBAHASAN

Data yang digunakan merupakan data publik yang dapat diakses oleh semua orang. Data ini berasal dari *CUISIDE dataset*. Data berupa gambar dari 2 kategori yakni gambar

yang bertumpuk dan data asli. Tabel 1 menunjukkan contoh dan sebaran dataset yang digunakan.

Arsitektur yang diusulkan untuk deteksi pemalsuan gambar menggunakan kombinasi *noiseprint* dan *ResNet-50* telah berhasil diimplementasikan dan dievaluasi. Hasil menunjukkan bahwa pendekatan ini mampu mencapai akurasi tinggi dalam membedakan gambar asli dengan gambar yang telah dimanipulasi. Kemudian, *Noiseprint* dihasilkan melalui kombinasi deteksi tepi dan penekanan *noise*. Deteksi tepi dilakukan menggunakan operator *Canny,* sedangkan penekanan *noise* diterapkan menggunakan operator *Laplacian*. Hasil dari kedua proses ini digabungkan untuk menghasilkan representasi *noiseprint*, yang mencerminkan karakteristik - unik dari setiap gambar. *Noiseprint* yang dihasilkan kemudian diekstraksi dan digunakan sebagai masukan untuk proses klasifikasi.

Model *ResNet-50,* yang merupakan salah satu arsitektur *deep learning* terlatih, digunakan untuk mengekstraksi fitur tingkat tinggi dari *noiseprint*. Dalam implementasinya, lapisan akhir (*fully connected layer*) pada *ResNet-50* dihilangkan untuk mendapatkan representasi fitur yang lebih kaya dan diskriminatif. Fitur-fitur yang diekstraksi mampu menggambarkan pola-pola kompleks dalam *noiseprint*, yang sulit diidentifikasi menggunakan metode manual. Tahap klasifikasi dilakukan menggunakan *Support Vector Machine (SVM). SVM* dilatih dengan *dataset* yang terdiri dari gambar asli dan gambar manipulasi, berdasarkan fitur yang diekstraksi oleh *ResNet-50*. Setelah proses pelatihan, *SVM* dapat memprediksi keaslian gambar baru dengan menganalisis fitur yang telah diekstraksi.

Kinerja arsitektur dievaluasi menggunakan *dataset* yang mencakup gambar asli dan manipulasi. Berdasarkan hasil evaluasi, arsitektur ini mampu mencapai akurasi sebesar 90.41% dalam mendeteksi gambar manipulasi. Tingginya akurasi ini menunjukkan efektivitas kombinasi *noiseprint* dan *ResNet-50* sebagai pendekatan deteksi pemalsuan gambar. Selain itu, model juga dievaluasi menggunakan metrik presisi, *recall, dan F1-Score.* Tabel 2 menunjukkan hasil dari evaluasi. Kemudian juga ditunjukkan *Confusion Matrix* dari proses pelatihan, seperti pada gambar 3.

Tabel 1
Contoh Dataset

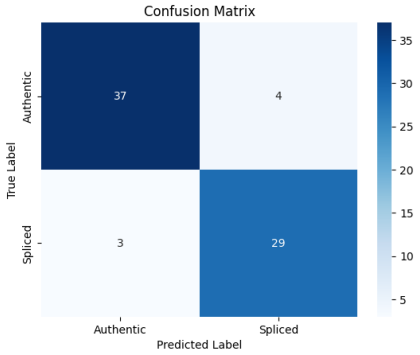
Data	Kategori	Jumlah
	Gambar asli	184
	Gambar ditumpuk	181

Sumber: Data Diolah

Tabel 2
Classification Report

Jenis	Precision	Recall	F1-score
Asli	0,93	0.90	0.91
Bertumpuk	0.99	0.91	0.89

Sumber: Data Diolah



Gambar 3. *Confusion Matrix*

Arsitektur yang diusulkan menunjukkan kinerja yang sangat baik dalam mendeteksi gambar manipulasi. *Noiseprint* terbukti efektif dalam menangkap karakteristik *noise* unik dari setiap gambar, yang berperan penting dalam membedakan gambar asli dan manipulasi. Di sisi lain, fitur tingkat tinggi yang diekstraksi oleh *ResNet-50* mampu mengenali pola-pola kompleks dalam *noiseprint*, memberikan representasi fitur yang kuat untuk klasifikasi. Kombinasi *noiseprint* dan *ResNet-50* dapat dijadikan sebagai pendekatan yang andal dalam mendeteksi pemalsuan gambar, dengan potensi pengembangan lebih lanjut untuk diterapkan pada berbagai domain aplikasi lainnya.

SIMPULAN

Penelitian ini menunjukkan bahwa gabungan *Noiseprint, ResNet-50*, dan *SVM* adalah solusi yang efektif untuk mendeteksi gambar palsu, terutama jenis *splicing. Noiseprint* terbukti dapat menangkap pola *noise* khas dari setiap gambar, sedangkan *ResNet-50* berhasil mengekstrak fitur penting dengan mendalam. Kombinasi ini memberikan akurasi yang cukup tinggi, yaitu 90,41%. Namun, metode ini masih perlu diuji lebih lanjut pada *dataset* yang lebih beragam dan nyata agar hasilnya lebih bisa diandalkan di berbagai kondisi. Meski ada beberapa tantangan, pendekatan ini sudah memberikan langkah besar untuk menangani masalah gambar palsu.

DAFTAR PUSTAKA

[1]. Wu, Y., Abd-Almageed, W., & Natarajan, P. (2018). BusterNet: Detecting copy-move image forgery with source/target localization. Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics), 11210 LNCS, 170–186. https://doi.org/10.1007/978-3-030-01231-1_11

[2]. Marpaung, F., Aulia, F., & Nabila, R. C. (2022). Computer Vision Dan Pengolahan Citra Digital. www.pustakaaksara.co.id

[3]. Solaiyappan, S., & Wen, Y. (2022). Machine learning based medical image deepfake detection: A comparative study. Machine Learning with Applications, 8(September 2021), 100298. https://doi.org/10.1016/j.mlwa.2022.100298
[4]. Fridrich, J. (2019). Digital forensics: Image authentication and forgery detection. IEEE Transactions on Information Forensics and Security, 14(1), 1-12. https://doi.org/10.1109/TIFS.2018.2876703
[5]. Zhang, K., Wang, Y., & Liu, X. (2021). A survey on image forgery detection methods based on deep learning. Artificial Intelligence Review, 54(2), 1-24. https://doi.org/10.1007/s10462-020-09801-8
[6]. Bhatia, S., Kumar, S., & Kumar, A. (2020). A survey on image forgery detection techniques: A comprehensive review. Multimedia Tools and Applications, 79(1), 1-26. https://doi.org/10.1007/s11042-019-08343-0
[7]. Saha, S., Roy, S., & Das, S. (2020). A comprehensive survey on image forgery detection techniques. Journal of Visual Communication and Image Representation, 75, 103032. https://doi.org/10.1016/j.jvcir.2020.103032
[8]. Khan, A., Khan, M. A., & Khan, M. A. (2020). Image forgery detection using deep learning: A comprehensive review. Journal of King Saud University - Computer and Information Sciences. https://doi.org/10.1016/j.jksuci.2019.01.007
[9]. Chen, Y., Zhang, Y., & Wang, S. (2019). Deep learning for image forgery detection: A survey. Journal of Computer Science and Technology, 34(2), 217-236. https://doi.org/10.1007/s11390-019-1925-7
[10]. Hussain, M., Ali, M., & Bhat, M. (2021). Image forgery detection using transfer learning and convolutional neural networks. Journal of Ambient Intelligence and Humanized Computing, 12(3), 3021-3030. https://doi.org/10.1007/s12652-020-02709-2