

BAB I

PENDAHULUAN

Bab ini membahas tentang latar belakang, rumusan masalah, tujuan, manfaat, ruang lingkup penelitian, serta sistematika penulisan pada skripsi “Klasifikasi Gambar Asli dan Palsu Menggunakan Teknik *Error Level Analysis* dan Arsitektur MobileNetV2”.

1.1 Latar Belakang

Saat ini, gambar telah menjadi salah satu bentuk media yang paling sering digunakan untuk menyampaikan informasi. Menurut data dari Google Search, sekitar 14 miliar foto dibagikan melalui media sosial setiap hari. Masifnya penyaluran informasi melalui gambar didukung oleh berbagai kemajuan teknologi seperti semakin efektifnya metode kompresi, cepatnya koneksi internet, serta berkembangnya aplikasi khusus yang didesain untuk membagikan foto dan gambar seperti Instagram dan Facebook (Passarella, 2012). Dengan berbagai interaksi yang terjadi secara digital, gambar dapat menjadi aspek krusial yang mampu menambahkan konteks atau bukti mengenai interaksi yang terjadi dalam lingkup digital (Zanardelli dkk., 2023). Sayangnya, banyak pihak yang menyalahgunakan aspek ini untuk tujuan tertentu dengan cara melakukan perubahan pada gambar untuk menyalurkan informasi yang palsu (Saber dkk., 2020).

Kemajuan teknologi memungkinkan pemalsuan gambar dilakukan dengan lebih mudah dan lebih sulit dikenali oleh mata manusia. *Software* seperti Adobe Photoshop dan GIMP memberikan kemudahan bagi siapa saja untuk menyunting gambar dengan berbagai fitur canggih yang ditawarkan. *Software* tersebut kini juga tersedia dalam versi *mobile* seperti Photoshop Express yang memungkinkan penyuntingan gambar secara cepat melalui *smartphone*. Penggunaan berbagai *software* pengolah gambar dapat memberikan manfaat seperti menambah nilai estetika dan kreativitas pada gambar. Misalnya seperti pemanfaatan *software* untuk keperluan penyuntingan gambar dalam pembuatan iklan produk agar dapat menarik calon konsumen.

Di sisi lain, *software* pengolah gambar dan teknik manipulasi gambar sering digunakan untuk mengendalikan konteks gambar untuk tujuan yang jahat seperti misinformasi (Thakur & Rohilla, 2020). Hal ini dilakukan dengan cara menambahkan atau menghilangkan informasi pada gambar sehingga terjadi perubahan pada struktur gambar yang menyebabkan informasi pada gambar menjadi tidak valid (Mehrdadi dkk., 2023)

Penyebaran misinformasi melalui pemalsuan gambar relatif mudah dilakukan karena manusia kesulitan mengenali perubahan visual pada gambar. Hal tersebut merupakan sebuah fenomena yang dikenal sebagai *change blindness cognitive effect*. Fenomena ini terjadi apabila mata manusia gagal untuk menyadari perubahan pada gambar ketika perubahan tersebut terjadi secara perlahan atau mata sedang fokus pada hal lain (Rensink dkk., 1997). *Change blindness cognitive effect* dapat mempengaruhi kemampuan manusia dalam mengidentifikasi elemen-elemen yang telah dimanipulasi dalam gambar. Menurut penelitian yang dilakukan oleh Nightingale dkk., (2017), dari sejumlah gambar asli dan termanipulasi, manusia hanya mampu mendeteksi sekitar 65% gambar termanipulasi. Performa ini hanya sedikit lebih tinggi dari peluang tebak acak yaitu sebesar 50%. Hal ini menunjukkan bahwa manusia memiliki kemampuan yang sangat terbatas dalam mengenali pemalsuan gambar. Dengan keterbatasan pemrosesan visual pada manusia serta maraknya kasus pemalsuan gambar, pengembangan sistem pengenalan pemalsuan gambar yang cepat dan akurat menjadi kebutuhan mendesak di bagi manusia.

Untuk mengatasi keterbatasan manusia dalam melakukan klasifikasi gambar asli dan palsu, dapat dikembangkan teknologi berbasis *machine learning* maupun *deep learning*. Teknologi ini memungkinkan sebuah model untuk melakukan tugas klasifikasi yakni mengelompokkan objek tertentu ke dalam kategori yang telah ditentukan (Kornyol dkk., 2023). Dalam topik ini, klasifikasi dapat digunakan untuk membedakan gambar dan mengelompokkannya ke dalam kelas asli dan termanipulasi, sebuah kasus klasifikasi biner. Dalam pembangunan model untuk melakukan tugas klasifikasi, diperlukan data berupa gambar sebagai data latih. Model dilatih sehingga dapat mempelajari fungsi yang akan memetakan *input* menjadi *output* berdasarkan data latih pasangan *input-output* dalam *dataset*, proses ini dinamakan *supervised learning* (Sarker, 2021).

Penelitian mengenai pembuatan model klasifikasi gambar palsu telah banyak dilakukan. Salah satu metode yang memiliki performa paling bagus adalah model dengan

arsitektur *deep learning*. Choudhary dkk., (2024), menggunakan arsitektur *Convolutional Neural Network* (CNN) dengan tiga lapisan untuk melakukan klasifikasi biner gambar asli dan palsu. Penelitian tersebut berhasil mengelompokkan gambar dengan performa yang cukup baik. Dilakukan juga proses segmentasi pada gambar yang dikenali sebagai gambar palsu. Barni dkk., (2017) menggunakan arsitektur CNN pada klasifikasi gambar asli dan palsu dengan kompresi JPEG sehingga mampu menghasilkan akurasi sebesar 81.7%. Beberapa penelitian ini menunjukkan bahwa model *deep learning* memiliki performa yang baik dalam kasus klasifikasi gambar asli dan palsu.

Dalam pembuatan model klasifikasi, dapat digunakan juga metode *transfer learning*. Metode ini memanfaatkan model *deep learning* yang telah dilatih pada *dataset* besar dan umum atau disebut model *pre-trained*. Model *pre-trained* ini kemudian disesuaikan untuk tugas yang lebih spesifik seperti klasifikasi gambar asli dan palsu. Dengan menggunakan *transfer learning*, waktu pembangunan dan pelatihan model bisa menjadi lebih efisien serta mencapai akurasi yang tinggi meskipun hanya dilatih dengan data yang terbatas (Z. Zhao dkk., 2024). Salah satu model *pre-trained* yang menawarkan simplisitas serta efisiensi memori pada penerapannya adalah MobileNet (Sandler dkk., 2018). Penelitian MobileNet dalam topik pengenalan gambar palsu dan asli telah dilakukan sebelumnya oleh Shikalgar dkk., (2023) yang menggunakan MobileNet versi pertama dan mampu mencapai akurasi tinggi yaitu sebesar 98.75%. Phan-Xuan dkk., (2019) kemudian menggunakan MobileNetV2 untuk melakukan tugas klasifikasi yang sama dan mampu mencapai akurasi sebesar 95.15% dengan model terbaru yang lebih ringan dari versi pertamanya. Dari penelitian tersebut, MobileNetV2 dapat dikembangkan untuk melakukan tugas klasifikasi gambar asli dan palsu sehingga menghasilkan model yang ringan dan mungkin dapat digunakan dalam platform *mobile*. Pengembangan ini akan mempermudah manusia dalam mengenali gambar asli dan palsu.

Untuk mempermudah model untuk mengenali perbedaan antara gambar asli dan manipulasi, dapat dilakukan proses ekstraksi fitur pada gambar. Proses ekstraksi fitur ini digunakan agar diperoleh informasi sebanyak mungkin pada data gambar (Mutlag dkk., 2020). Beberapa teknik yang dapat digunakan dalam pengenalan gambar asli dan palsu antara lain ELA, SURF, serta *patch* YcrCb. Teknik ekstraksi fitur yang digunakan dalam pengenalan manipulasi pada gambar berformat *lossy* adalah *error level analysis* (ELA). Penelitian yang dilakukan oleh Choudhary dkk., (2024) menunjukkan bahwa teknik ELA

yang digabungkan dengan *shallow* CNN cukup efektif dalam melakukan *task* klasifikasi gambar asli dan palsu dengan akurasi mencapai 91.70%. Teknik ini bekerja dengan cara mengidentifikasi area dengan perbedaan kompresi pada setiap *channel* gambar yang kemudian akan digabungkan menjadi gambar ELA. Dengan menggunakan ELA, variasi halus pada gambar yang telah diubah dapat ditangkap dengan lebih akurat (Jia dkk., 2024). Setelah fitur ELA dibuat, fitur tersebut dapat digunakan sebagai *input* dalam arsitektur *deep learning*. Meskipun pada model *deep learning* proses ekstraksi fitur biasanya sudah dilakukan secara otomatis, seperti melalui layer konvolusi pada CNN, memasukkan fitur ELA sebagai tambahan dapat memberikan informasi ekstra yang mungkin tidak dapat ditangkap secara baik oleh model. Melalui pendekatan ini, peneliti akan melakukan penggabungan antara model *deep learning pre-trained* MobileNetV2 dengan fitur ekstraksi berupa ELA untuk melakukan klasifikasi gambar asli dan palsu. Penelitian ini diharapkan dapat menghasilkan model ringan yang mampu melakukan klasifikasi manipulasi gambar sehingga dapat diterapkan pada perangkat dengan sumber daya yang terbatas seperti perangkat *mobile*.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah diuraikan pada bagian sebelumnya, dapat dirumuskan permasalahan yang dibahas pada penelitian ini yaitu bagaimana melakukan klasifikasi biner gambar palsu dan asli dengan menggunakan teknik ekstraksi fitur berupa *error level analysis* (ELA) dan arsitektur MobileNetV2.

1.3 Tujuan dan Manfaat

Tujuan umum dari penelitian ini adalah mendapatkan model klasifikasi gambar asli dan palsu menggunakan MobileNetV2 dan teknik ekstraksi fitur ELA. Adapun tujuan khusus dari penelitian ini adalah untuk menganalisis performa teknik ELA pada model MobileNetV2 dalam melakukan klasifikasi gambar asli dan palsu.

Manfaat dari penelitian ini adalah didapatkannya model sistem klasifikasi gambar asli dan palsu yang dapat berguna pada bidang *digital forensic* sehingga meningkatkan keamanan digital melalui pencegahan penyebaran misinformasi.

1.4 Ruang Lingkup

Dalam penelitian ini, diterapkan batasan-batasan sebagai ruang lingkup penelitian agar penelitian yang dilakukan menjadi lebih terarah dan dapat mencapai tujuan yang diharapkan.

Ruang lingkup dari penelitian ini mencakup:

1. Penelitian dilakukan menggunakan Google Colab sebagai lingkungan untuk melakukan pemrosesan data serta pelatihan model.
2. Data yang digunakan pada penelitian ini adalah data CASIA 2.0 dengan dua kategori kelas yaitu gambar asli dan gambar palsu.
3. Model yang digunakan pada penelitian ini adalah model MobileNetV2 yang dibangun dengan *library* keras.
4. *Hyperparameter* terbaik yang akan ditentukan adalah pemilihan nilai *dropout*, jumlah neuron yang dilatih kembali (*unfreeze*) selama proses pelatihan, serta *optimizer* pada model.
5. Evaluasi kinerja model dilakukan dengan menganalisis hasil akurasi, presisi, serta *recall* dari model yang telah dilatih.

1.5 Sistematika Penulisan

Penyusunan laporan penelitian ini disesuaikan dengan sistematika penulisan untuk memberikan gambaran mengenai proses penelitian yang dilakukan. Sistematika penulisan laporan penelitian ini adalah sebagai berikut:

BAB I PENDAHULUAN

Bab ini membahas mengenai latar belakang penelitian yang dilakukan, rumusan masalah yang didapat, ruang lingkup dari penelitian, tujuan dan manfaat penelitian, serta sistematika penulisan laporan yang dibuat.

BAB II LANDASAN TEORI

Bab ini menjelaskan berbagai teori yang digunakan dalam penelitian klasifikasi gambar asli dan palsu dengan menggunakan teknik ELA dan arsitektur MobileNetV2.

BAB III METODOLOGI PENELITIAN

Bab ini menjelaskan tentang metodologi yang digunakan dalam penelitian klasifikasi gambar asli dan palsu menggunakan teknik ELA dan arsitektur MobileNetV2.

BAB IV HASIL DAN PEMBAHASAN

Bab ini menjelaskan mengenai analisis dan hasil penelitian mengenai klasifikasi gambar asli dan palsu menggunakan teknik ELA dan arsitektur MobileNetV2.

BAB V KESIMPULAN

Bab ini berisi tentang kesimpulan dari penelitian yang dilakukan serta saran untuk pengembangan penelitian lebih lanjut.