BAB I

PENDAHULUAN

1.1. Latar Belakang

Perkembangan teknologi telah merevolusi kegiatan pengambilan dan distribusi foto. Dalam era digital ini, kegiatan pengambilan foto dapat diakses dengan mudah melalui gawai seperti *smartphone* yang memiliki kamera, dan disimpan dalam bentuk digital. Sebuah estimasi menyatakan bahwa pada tahun 2020 saja, telah dibuat hingga 1,4 miliar foto digital [1]. Foto-foto atau gambar digital tersebut dapat didistribusikan dengan mudah secara terbuka dalam skala internasional melalui internet, contohnya dengan menggunakan media sosial. Menurut datareportal, pada Juli 2023, ada 15 platform media sosial yang memiliki setidaknya 400 juta pengguna aktif, dan 7 platform media sosial yang memiliki setidaknya 1 miliar pengguna aktif per bulan, di antaranya adalah Facebook, YouTube, WhatsApp, dan Instagram, yang semuanya sering digunakan untuk mendistribusi gambar digital [2]. Banyak media sosial ini memiliki konten yang bertipe *user generated content* (UGC), dan menjadi salah satu sarana yang paling sering digunakan dalam menyebarkan gambar-gambar digital. Konten bertipe UGC dibuat oleh pengguna - pengguna reguler dari media sosial secara suka rela, sehingga konten memiliki variasi dan volume yang sangat tinggi dan sulit untuk dibatasi atau dipantau secara keseluruhan [3].

Kemudahan akses, distribusi, dan kesulitan kegiatan pemantauan terhadap gambar digital ini mendorong peningkatan jumlah dan peredaran gambar digital yang sangat pesat. Banyaknya pengguna juga mendorong kemajuan teknologi pada bidang aplikasi *editing* foto. Seiring berjalannya waktu, aplikasi *editing* foto semakin canggih dan mudah diakses oleh khalayak umum, contohnya aplikasi seperti Adobe Photoshop, Adobe Lightroom, Picsart, dan banyak aplikasi lain yang umumnya memiliki sumber yang terbuka dan gratis [4]. Sayangnya,

perkembangan-perkembangan ini juga meningkatkan risiko pemalsuan gambar yang berdampak negatif.

Foto merupakan komoditas penting dalam komunikasi. Foto memiliki peran vital dalam menyampaikan informasi. Foto-foto sering digunakan sebagai bukti atau referensi dalam berbagai konteks seperti jurnalisme, hukum, dan forensik [5]. Oleh karena itu, pemalsuan foto dapat memiliki dampak negatif yang serius pada integritas informasi. Menurut kementrian komunikasi dan informasi (Menkominfo), pada triwulan pertama tahun 2023 telah ditemukan 495 isu integritas informasi atau hoaks pada platform digital. Jumlah ini meningkat dari triwulan tahun sebelumnya yang mencapai 393 isu hoaks. Total, menkominfo telah menemukan sebanyak 11.357 isu hoaks di Indonesia pada tahun 2018 hingga 2023 dalam berbagai bidang [6].

Salah satu upaya pencegahan terhadap ancaman integritas informasi akibat manipulasi atau pemalsuan foto adalah dengan mempelajari teknik-teknik deteksi pemalsuan foto. Teknik deteksi pemalsuan foto dapat dibagi menjadi kategori aktif dan pasif [7]. Dalam metode aktif, sebuah *watermark* atau tanda tangan digital dibuat dalam foto atau gambar untuk mencegah pemalsuan [8]. Keberadaan watermark atau tanda tangan ini yang dideteksi untuk memastikan keaslian gambar. Namun, metode ini kurang praktis dan tidak dapat diterapkan dalam segala situasi, contohnya ketika gambar asli tidak memiliki *watermark* atau tanda tangan di dalamnya [9]. Deteksi pasif tidak memiliki keterbatasan yang dialami deteksi aktif, karena deteksi pasif mendeteksi keberadaan manipulasi yang dilakukan ke gambar palsu. Oleh karena itu, pendekatan menggunakan deteksi pasif lebih sering dilakukan. Dua teknik manipulasi yang sering digunakan adalah *splicing* dan *copy-move forgery* (CMF) [10]. Dalam teknik *splicing*, konten dari beberapa gambar dimanipulasi dan disatukan dalam satu gambar.

Teknik CMF mengambil suatu daerah atau bagian dari suatu gambar untuk disalin dan ditempelkan pada bagian lain dari gambar yang sama. Teknik ini merupakan salah satu teknik manipulasi gambar yang paling sering dan mudah

untuk digunakan [11]. Karena berasal dari gambar yang sama, tekstur pada bagian yang disalin sama dengan foto secara keseluruhan [12]. Hal ini memungkinkan penipuan yang sulit terdeteksi yang mengancam keandalan informasi visual. Pendekatan *copy-move forgery detection* (CMFD) dapat dibagi menjadi pendekatan *deep learning-based* dan *handcrafted-based* [13]. Dalam pendekatan dalam *handcrafted-based* ada yang berbasis blok, berbasis keypoints, dan pendekatan hybrid. *Deep learning-based* menggunakan arsitektur model yang dibuat sendiri dari awal, atau dengan memodifikasi model dari arsitektur yang telah dilatih sebelumnya, contohnya seperti VGG-16 [14]. Penelitian menunjukkan pendekatan *deep learning-based* memberikan hasil yang lebih baik dan menjanjikan disbanding pendekatan *handcrafted-based*. Pendekatan *handcrafted-based* memiliki keterbatasan dalam klasifikasi untuk data yang sangat besar karena bergantung pada pencarian pola yang ditentukan secara manual, berkaitan dengan konten yang terduplikasi. Oleh karena itu, peneliti memilih pendekatan *deep-learning* dalam mengembangkan solusi yang efektif untuk mendeteksi pemalsuan foto [15].

Deep learning mencakup banyak metode dan arsitektur. Contohnya ada *Recurrent Neural Networks* (RNN), *Generative Adversarial Networks* (GAN), *Convolutional Neural Networks* (CNN), dan lainnya. Setiap metode memiliki keunggulan dan kelemahan masing-masing. Pada penelitian ini, dipilih metode *deep learning* CNN karena efektivitasnya dalam analisa dan deteksi objek gambar. *Convolutional layers* pada CNN dapat mengurangi dimensi gambar yang tinggi tanpa menghilangkan informasi yang dimiliki gambar [16]. CNN memiliki kelebihan dalam mempelajari pola atau tekstur lokal dan mengidentifikasi kesamaan atau inkonsistensi dalam sebuah gambar. Selain itu, CNN juga memiliki banyak jenis model yang telah dilatih sebelumnya, sehingga memberikan kemudahan dalam proses optimasi. Kelebihan-kelebihan yang ditawarkan oleh algoritma CNN membuatnya cocok untuk digunakan dalam penelitian untuk mengoptimasi model deteksi dan lokalisasi manipulasi gambar menggunakan *copy-move*. [17]

Hasil dari penelitian ini diharapkan dapat memberikan sumbangan penting dalam perkembangan teknologi forensik digital. Para profesional forensik dan penegak hukum akan mendapatkan alat yang lebih kuat dalam melacak bukti digital yang sah. Selain itu, penelitian ini juga dapat membantu platform media sosial dan situs web berita dalam menjaga keaslian konten yang diunggah oleh pengguna, yang merupakan langkah penting dalam memerangi disinformasi dan penyebaran berita palsu yang merugikan masyarakat luas. Dengan demikian, penelitian ini memiliki dampak signifikan dalam menjaga integritas gambar digital dan informasi yang dikonsumsi dalam era digital ini.

Program MBKM Penelitian bertujuan menghasilkan publikasi yang memberikan kontribusi ilmiah. Penelitian dilakukan dari Juli hingga Desember 2023, bersama dengan tim penelitian yang beranggotakan pemimpin penelitian dan 5 anggota penelitian. Topik besar yang diangkat dalam penelitian ini adalah sistem deteksi pemalsuan gambar digital berbasis *machine learning* dan *deep learning*. Topik besar dipecah menjadi beberapa topik spesifik, dua diantaranya adalah optimasi model deteksi pemalsuan copy-move pada gambar digital menggunakan CNN, dan optimasi model lokalisasi pemalsuan *copy-move* pada gambar digital menggunakan CNN. Target luaran kegiatan MBKM penelitian ini adalah publikasi konferensi. Topik deteksi pemalsuan *copy-move* memiliki target publiksi untuk konferensi ICMERALDA 2023 yang diadakan pada 24 hingga 25 November 2023 secara virtual, dan topik lokalisasi pemalsuan copy-move memiliki target publikasi untuk konferensi IAICT 2024 yang diadakan pada tanggal 4 hingga 6 Juli 2024 di Bali. Kedua topik penelitian dilakukan menggunakan kerangka kerja menggunakan metode yang didasari *framework Knowledge Discovery in Databases* (KDD)

1.2. Rumusan Masalah

1. Apakah dengan menggunakan metode *deep learning convolutional neural network* dapat meningkatkan akurasi deteksi pemalsuan gambar *copy-move*?

2. Apakah dengan melakukan optimasi *hyperparameter* dapat meningkatkan akurasi deteksi pemalsuan gambar *copy-move*?
3. Apakah dengan menggunakan metode *deep learning* dapat meningkatkan akurasi model lokalisasi pemalsuan gambar *copy-move*?

1.3.Tujuan Penelitian

1. Optimasi model deteksi pemalsuan gambar *copy-move* menggunakan metode *deep learning*, yaitu CNN.
2. Meningkatkan akurasi model deteksi pemalsuan gambar *copy-move* di atas 90%.
3. Optimasi model lokalisasi pemalsuan gambar *copy-move* dengan teknik *deep learning* untuk meningkatkan akurasi lokalisasi pemalsuan gambar *copy-move*.

1.4.Urgensi Penelitian

1. Peningkatan drastis akan gambar digital yang beredar, gambar digital menjadi salah satu sarana paling umum dan vital dalam distribusi informasi.
2. Manipulasi gambar digital yang semakin mudah karena kemajuan teknologi untuk editing gambar, meningkatkan banyak gambar palsu yang beredar di masyarakat.
3. Menjaga integrasi informasi di tengah peningkatan peredaran hoaks dari pemalsuan gambar digital.

1.5.Luaran Penelitian

1. Konferensi *International Conference on Modeling and E-Information Research, Artificial Learning and Digital Applications* (ICMERALDA) 2023 di Karawang, Jawa Barat, Indonesia. Dilaksanakan pada tanggal 24-25 November 2023 secara virtual.
2. Konferensi *The 2024 IEEE International Conference on Industry 4.0, Artificial Intelligence, and Communication Technology* (IAICT 2024) di Bali, Indonesia. Dilaksanakan pada tanggal 4-6 Juli 2024.

1.6.Manfaat Penelitian

1. Membantu mendeteksi foto palsu yang telah dimanipulasi menggunakan teknik *copy-move*.
2. Membantu lokalisasi bagian yang terkena manipulasi teknik *copy-move* pada foto palsu.
3. Membantu dalam mengurangi misinformasi yang terjadi akibat pemalsuan foto yang menggunakan teknik *copy-move*.
4. Menjadi referensi dalam penelitian lebih lanjut akan deteksi pemalsuan foto.