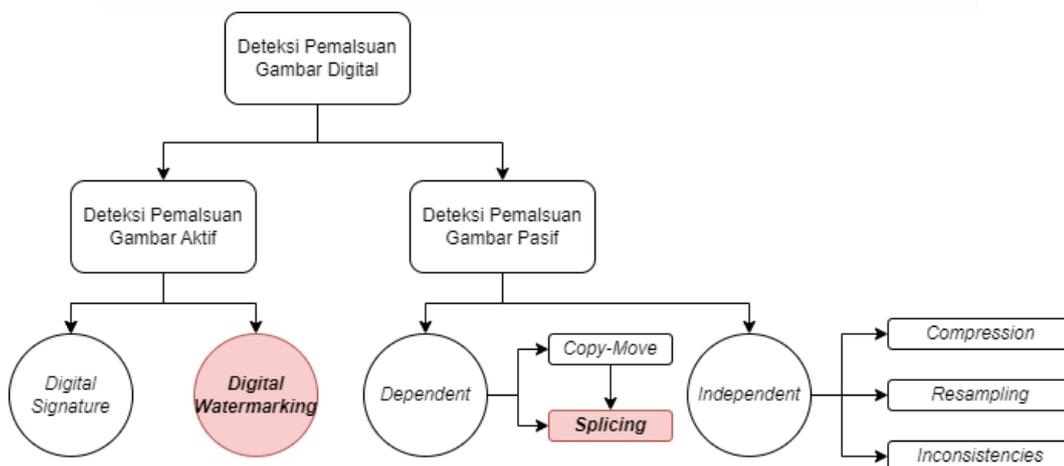


BAB I

PENDAHULUAN

1.1. Latar Belakang

Revolusi industri keempat membuat komunikasi melalui *platform* multimedia semakin sederhana, efisien, dan efektif karena perkembangan internet [1]. Aktivitas pemalsuan gambar sedang marak terjadi karena perkembangan teknologi multimedia yang membuat teknologi *editing* gambar semakin canggih dan mudah digunakan. Namun, tidak semua aktivitas pemalsuan gambar dimaksudkan untuk hal yang positif. Banyak pemalsuan gambar dimanfaatkan untuk memfitnah orang, mendapatkan keuntungan finansial melalui pemerasan, dan tindakan kriminal lainnya [2]. Sistem pendeteksi pemalsuan gambar memiliki dua teknik yang berbeda, yaitu deteksi aktif dan deteksi pasif. Salah satu teknik deteksi aktif adalah melalui *digital watermark* pada gambar. Sedangkan, untuk deteksi pasif bisa dilakukan dengan deteksi *splicing* pada gambar [3]. Gambar 1.1 menunjukkan diagram klasifikasi teknik deteksi pemalsuan gambar digital.



Gambar 1.1 Klasifikasi teknik pemalsuan gambar digital [3]

Pada teknik deteksi aktif melalui *watermark*, informasi akan ditanamkan pada gambar menggunakan teknik enkripsi untuk menanamkan dan dekripsi untuk mengekstrak informasi keasliannya. Teknik enkripsi dan dekripsi ini bisa dilakukan dengan menggunakan algoritma *deep learning* [4]. *Digital watermarking* adalah

sebuah proses mengimplementasikan sebuah tanda unik terhadap sebuah data digital untuk mencegah pemalsuan. Seiring dengan perkembangan data digital, proses memisahkan data *watermark* dan tidak *watermark* membutuhkan banyak waktu [5]. *Watermark* mempunyai kualitas ketahanan yang baik karena bisa menahan bentuk-bentuk manipulasi, seperti pemotongan, rotasi, dan lain-lain [6]. Apalagi, secara visual manusia sulit untuk membedakan mana gambar yang sudah dimodifikasi dan mana yang masih original. Oleh karena itu, penting untuk mengotomasi proses identifikasi apakah sebuah gambar memiliki *watermark* atau tidak [5].

Teknik deteksi pasif banyak digunakan untuk mengatasi pemalsuan gambar, khususnya yang dilakukan dengan teknik *splicing*. Oleh karena itu, pada deteksi pasif, yang dideteksi adalah teknik pemalsuan yang ada pada gambar. *Splicing* adalah sebuah metode pemalsuan gambar dengan menggabungkan dua gambar atau lebih menjadi satu gambar utuh yang baru [7]. Terkadang, manusia tidak menyadari bahwa gambar yang mereka lihat adalah gambar yang sudah dipalsukan. Oleh karena itu, automasi proses identifikasi *splicing* pada gambar juga perlu dilakukan.

Perkembangan teknologi saat ini juga berperan dalam mempopulerkan model *deep learning* sehingga model-model yang dihasilkan lebih fungsional dengan akurasi yang cukup memuaskan. Model-model tersebut akhirnya mampu bertransformasi secara masal karena integrasi kecerdasan dan akhirnya membentuk beberapa seperti jaringan sosial, transportasi otomatis, manufaktur otomatis, *language processing*, *intelligence warfare*, dan *smart health* [8]. Seiring berjalannya waktu, *deep learning* mencapai level akurasi yang lebih tinggi dibandingkan biasanya. Kemajuan ini membuat *deep learning* krusial untuk menjaga keamanan dan membantu pengguna memenuhi ekspektasi mereka [9]. Salah satu algoritma *deep learning* yang bisa dimanfaatkan untuk mendeteksi *digital watermark* dan *splicing* pada gambar adalah *convolutional neural network* (CNN). CNN adalah algoritma *deep learning* yang paling populer dan banyak digunakan saat ini [10]. Selain itu, dibandingkan dengan algoritma *deep learning* lainnya, CNN adalah yang paling efektif untuk memahami data gambar [11].

Populernya CNN disebabkan oleh beberapa kelebihan yang ditawarkan, seperti CNN bisa mendeteksi *feature* penting secara otomatis tanpa pengawasan manusia, tergolong cukup efisien, dan bisa dijalankan diberbagai macam perangkat [6]. Berdasarkan keuntungan yang sudah dijabarkan diatas, maka penelitian ini menggunakan algoritma *deep learning* CNN untuk mendeteksi pemalsuan gambar berdasarkan *digital watermark* dan *splicing*.

1.2. Rumusan Masalah

Penelitian ini memiliki rumusan masalah sebagai berikut:

1. Apakah dengan menggunakan algoritma CNN hasil akurasi deteksi *splicing* gambar pada *dataset* DVMM cukup memuaskan?
2. Apakah dengan menggunakan algoritma CNN hasil akurasi deteksi gambar palsu berdasarkan *digital watermark* lebih akurat daripada menggunakan *transfer learning*?
3. Apakah dengan melakukan optimasi pada model CNN deteksi gambar palsu berdasarkan *digital watermark* bisa meningkatkan akurasi?

1.3. Tujuan Penelitian

Penelitian ini memiliki tujuan sebagai berikut:

1. Menghasilkan model CNN pendeteksi *splicing* gambar pada *dataset* DVMM.
2. Menghasilkan model CNN pendeteksi pemalsuan gambar berdasarkan *digital watermark*.
3. Mengoptimasi model CNN pendeteksi pemalsuan gambar berdasarkan *digital watermark* untuk meningkatkan akurasi model.

1.4. Urgensi Penelitian

Urgensi penelitian ini adalah sebagai berikut:

1. Banyaknya kasus kriminalitas akibat pemalsuan foto karena kemajuan teknologi alat *editing* gambar.
2. Membantu membedakan informasi yang asli dan palsu berdasarkan *watermark* dan deteksi *splicing* pada gambar.

1.5. Luaran Penelitian

Penelitian ini akan dipublikasikan pada Journal of Applied Science and Engineering Published by Tamkang University Press yang terindeks Scopus Q2. Judul publikasi yang telah di-submit adalah “*Enhancing Convolutional Neural Network Models for Detecting Watermarked Images*”.

1.6. Manfaat Penelitian

Manfaat penelitian ini pada bidang edukasi, diantaranya adalah sebagai berikut:

1. Menghasilkan model yang mampu mendeteksi *splicing* pada gambar untuk membedakan gambar asli dan palsu.
2. Menghasilkan model yang sudah dioptimasi untuk mendeteksi *digital watermark* pada gambar untuk mencegah penyebaran informasi palsu melalui gambar digital.