

BAB I

PENDAHULUAN

1.1 Latar Belakang

Selaras dengan teknologi pengolahan media digital yang semakin maju, manipulasi video dapat dilakukan dengan mudah. Tersedia banyak aplikasi rekayasa video dengan teknologi beragam yang menyediakan kemudahan bagi seseorang untuk melakukan manipulasi video sesuai dengan kebutuhan. Beberapa diantaranya adalah *Capcut*, *Filmora*, *Adobe Premiere Pro*, *Vegas Pro*, *DaVinci Resolve*, dan lain sebagainya (A. I. Putra dkk., 2021). Mengubah citra yang terekam dalam video memunculkan tantangan dalam membedakan realitas dan fiksi. Proses mengubah isi video dengan tujuan untuk menyembunyikan suatu objek, peristiwa atau mengubah makna yang disampaikan oleh gambar dalam video dinamakan *video tampering* (Sitara dan Mehtre, 2016). Salah satu tantangan paling besar dalam *video tampering* adalah penggunaan *deepfake*, yang menggunakan algoritma machine learning untuk menciptakan video palsu yang sulit dibedakan dari video asli. *Deepfake* merupakan salah satu bentuk kecerdasan buatan yang memanfaatkan algoritma *machine learning* untuk memanipulasi file media yang ada kemudian ditiru untuk membuat duplikasinya (Wibowo dkk., 2023). Di samping teknik *deepfake*, terdapat teknik manipulasi video lain seperti, *video splicing*, *color grading manipulation*, *cropping* dan lain-lain. Teknik-teknik tersebut mempunyai tujuan yang sama yaitu untuk memanipulasi citra visual dalam video dengan cara tertentu.

Di balik kemudahan dari beragamnya teknik dan teknologi untuk mengubah video, terdapat konsekuensi serius dalam konteks penyebaran informasi palsu hingga konsekuensi hukum. Video *tampering* berpotensi untuk meningkatkan penyebaran disinformasi, propaganda politik, pencemaran nama baik, penipuan, pemerasan, pornografi, dan mempengaruhi proses pengambilan keputusan (Kasita, 2022). Saat ini, pendeteksian manipulasi video masih menghadapi tantangan besar karena banyaknya teknik manipulasi canggih yang sulit dideteksi dengan metode konvensional. Dalam konteks hukum, integritas bukti dalam investigasi dan persidangan dapat terganggu oleh tindakan manipulasi video (Riadi dkk., 2023). Hal ini terjadi karena video *tampering* dapat menimbulkan keraguan terhadap kebenaran peristiwa yang terekam dalam video. Manipulasi video dapat merusak kepercayaan publik dan berdampak signifikan terhadap masyarakat (Akhtar dkk., 2022).

Pemastian keaslian dan integritas video yang digunakan sebagai sumber informasi salah satunya dapat dilakukan dengan pendeteksian *video tampering*. Deteksi manipulasi video sangat penting untuk melindungi keamanan individu dan lembaga dari berbagai masalah yang dapat timbul dari adanya video *tampering*. Teknologi deteksi manipulasi citra terus berkembang memungkinkan untuk membedakan antara video asli dan yang telah dimanipulasi. Deteksi manipulasi video dapat dilakukan diantaranya dengan cara analisis metadata, analisis *hash*, dan analisis secara visual atau analisa *frame* (Al-Azhar, 2012). Analisis video secara visual dilakukan dengan menggunakan metode dan teknik khusus untuk memahami konten visual dari video. Secara umum, metode yang digunakan untuk mendeteksi

video diklasifikasikan menjadi dua kategori; kategori pertama adalah *tampering detection*, yaitu metode deteksi yang hanya memvalidasi keaslian video secara keseluruhan tanpa memberikan informasi tentang bagian video yang telah dimanipulasi; kategori kedua adalah *tampering localization*, yaitu metode deteksi yang menunjukkan lokasi hasil manipulasi pada video (Sari dkk., 2017).

Secara teknis, video terdiri dari kumpulan gambar (*frame*) yang dibaca berurutan dengan jumlah tertentu tiap detik yang menunjukkan tindakan berkesinambungan dalam urutan gambar (Widiarto, 2016). *Frame-frame* tersebut dapat diperiksa dengan *tampering localization* untuk mendeteksi tindakan *tampering* yang mungkin terjadi dalam video tersebut. Jika terdapat *frame* yang mengindikasikan manipulasi, dapat diambil kesimpulan bahwa video tersebut telah mengalami *tampering* (Sari, 2020). Terdapat berbagai metode deteksi manipulasi gambar, diantaranya adalah metode *Error Level Analysis* (ELA) yang menganalisis gambar melalui berbagai tingkat kompresi. Metode ELA bekerja dengan cara melakukan perbandingan antara tingkat kesalahan piksel pada gambar asli dengan tingkat kesalahan piksel pada gambar yang telah dimodifikasi atau disimpan ulang (Purnama dkk., 2023; Wicaksono dkk., 2022). Metode *Speed Up Robust Features* (SURF) yang merupakan sebuah metode deteksi fitur menggunakan *keypoint* dari sebuah gambar citra. Dalam mendeteksi manipulasi gambar, metode SURF bekerja dengan membandingkan dua gambar (gambar asli dan gambar yang diduga dimanipulasi) dan menghasilkan garis yang menghubungkan *keypoint* yang cocok (Lubis dkk., 2016; Sulistyio dkk., 2020). Selain itu terdapat metode *Scale-Invariant Feature Transform* (SIFT) yang cara kerjanya hampir sama dengan metode SURF,

yaitu mendeteksi fitur khusus dalam suatu gambar kemudian didapat nilai *keypoint* dari dua gambar yang diuji. Hasil *keypoint* tersebut dibandingkan dan dianalisis kecocokan objeknya (Rosidin dkk., 2018; Saputro & Prayudi, 2022).

Beberapa metode tersebut digunakan untuk menentukan lokasi gangguan pada gambar namun metode tersebut tidak dapat diterapkan pada video secara langsung karena perbedaan mendasar antara gambar statis dan video (Akhtar dkk., 2022a). Adanya *Localization Tampering* memberikan solusi terhadap permasalahan yang tidak dapat diselesaikan dengan metode deteksi manipulasi gambar. Teknik ini memungkinkan untuk mengidentifikasi *frame* tertentu di mana manipulasi terjadi, namun *Localization Tampering* memiliki keterbatasan karena hanya menunjukkan *frame* yang terindikasi manipulasi tanpa memberikan visualisasi area yang mengalami perubahan pada *frame* tersebut. Disinilah metode deteksi manipulasi gambar seperti *Error Level Analysis* berperan melengkapi kekurangan tersebut. Metode *Error Level Analysis* dapat mengidentifikasi perbedaan tingkat kesalahan kompresi antara gambar asli dan gambar hasil manipulasi. Hal ini meliputi area yang mungkin tidak dapat dideteksi oleh mata manusia atau oleh metode konvensional, dengan begitu *Error Level Analysis* mampu mengidentifikasi manipulasi yang paling halus sekalipun (Al-Fajri dkk., 2021a).

Dalam pendeteksian *tampering* pada video, metode *Localization Tampering* dan *Error Level Analysis* dikombinasikan untuk mengidentifikasi bagian-bagian yang mungkin telah dimanipulasi dalam video. *Localization Tampering* fokus pada deteksi perubahan pada area tertentu dalam video sehingga dapat memberikan informasi lokasi *frame* terjadinya *tampering*. *Error Level Analysis* bekerja dengan

mendeteksi tingkat kesalahan kompresi pada gambar dan menunjukkan area manipulasi pada *frame*. Dengan mengkombinasikan kedua metode ini, penelitian diharapkan mampu memberikan analisis yang lebih mendalam dalam mendeteksi manipulasi pada video digital.

Penelitian sebelumnya telah banyak mengkaji metode *Localization Tampering* dan *Error Level Analysis* secara terpisah dalam mendeteksi manipulasi gambar atau video dan sering kali mengalami kesulitan dalam mendeteksi manipulasi berlapis atau kompleks yang menggabungkan beberapa teknik manipulasi secara bersamaan (Akhtar dkk., 2022b). Berdasarkan uraian latar belakang tersebut, penelitian ini akan melakukan pendeteksian *tampering* pada video. Penelitian ini menggunakan sampel video digital asli dan video digital asli yang telah mengalami *tampering*. Penelitian berfokus pada forensik video dengan melakukan analisis perbandingan pada kedua video yang nantinya akan diketahui bahwa terdapat *tampering* yang diterapkan pada salah satu video. Penelitian memanfaatkan metode *Localization Tampering* dalam pemeriksaan antar *frame* untuk mengetahui detail informasi lokasi terjadinya *tampering* pada video, kemudian penggunaan metode *Error Level Analysis* (ELA) untuk mendeteksi area *tampering* pada *frame-frame* tertentu yang diindikasikan telah terjadi manipulasi. Penelitian ini menawarkan pendekatan gabungan yang memanfaatkan keunggulan masing-masing metode, sehingga diharapkan dapat memberikan hasil deteksi dan visualisasi manipulasi yang lebih informatif.

Penelitian ini memiliki keterbatasan dalam hal ketersediaan data, di mana metode yang digunakan memerlukan video asli sebagai referensi pembandingan.

Tanpa adanya video asli, proses deteksi manipulasi tidak dapat dilakukan karena kedua metode bergantung pada analisis perbandingan antara video asli dan video yang diduga telah mengalami tampering.

Penelitian ini bertujuan untuk mendalami bidang forensik terutama pada bagian citra digital berupa video dengan memfokuskan upaya ada teknik analisis manipulasi visual, sehingga dapat digunakan dalam mendukung investigasi forensik.

1.2 Rumusan Masalah

Berdasarkan latar belakang yang telah dijelaskan, maka rumusan masalah yang akan dikaji dalam penelitian ini adalah bagaimana mengkombinasikan metode *Localization Tampering* dan *Error Level Analysis* (ELA) dalam satu alur proses untuk mendeteksi video serta memberikan visualisasi area yang dimanipulasi?

1.3 Tujuan Penelitian

Berdasarkan rumusan masalah yang telah dipaparkan, maka tujuan dari penelitian ini adalah untuk mengkombinasikan metode *Localization Tampering* dan *Error Level Analysis* (ELA) dalam satu alur proses yang dapat mendeteksi manipulasi video serta memberikan visualisasi area yang dimanipulasi.

1.4 Manfaat Penelitian

Manfaat dari penelitian video *tampering* ini adalah sebagai berikut:

1. Manfaat untuk umum, dapat memberikan pembelajaran dan pengetahuan dalam menganalisa keaslian sebuah video.
2. Manfaat untuk Universitas Siliwangi, sebagai bahan pengembangan pengetahuan ilmiah, terutama dalam program studi Informatika.
3. Manfaat untuk bidang keilmuan, sebagai sumbangan pemikiran dan pengetahuan pendeteksian dan analisis *tampering* pada video, serta dapat menjadi sumber rujukan dan referensi ilmiah di bidang forensik dan keamanan digital dalam memahami dan mengatasi manipulasi video.
4. Manfaat untuk penulis, dapat menambah wawasan keilmuan teori maupun praktek terkait analisis video *tampering*.

1.5 Batasan Masalah

Terdapat beberapa batasan masalah dari penelitian ini, diantaranya sebagai berikut:

1. File video yang digunakan dalam penelitian ini diambil dari situs web *Pexels* (<https://www.pexels.com/id-id/video/mode-wanita-kedudukan-putih-9558963/>) dengan durasi 5 detik untuk keperluan penelitian.
2. File video yang digunakan dalam penelitian ini sebanyak 4 buah file video (1 buah video asli dan 3 buah video yang sudah dilakukan *tampering*), masing-masing berdurasi 5 detik.
3. Tipe citra yang akan dijadikan sampel untuk uji coba adalah file video berekstensi MP4 yang diekstrak menjadi file gambar berformat .PNG (*Portable Network Graphics*).

4. Simulasi pada video hanya dilakukan dengan *attack tampering* spasial berjenis *splicing*, berupa *face swap*, *superimposing*, dan penyisipan objek.
5. Pengembangan metode dilakukan dengan menggunakan menggunakan *Python* dan *Matlab*.
6. Analisis tingkat kesalahan (ELA) dilakukan dengan menggunakan *tools Forensically Beta*.
7. Penerapan *tampering* video dilakukan menggunakan aplikasi CapCut di *smartphone*, dan penelitian tidak mencakup prosedur forensik pada perangkat tersebut.