(Octavia & Movanita, 2024). Adapun contoh kasus lain yang menggunakan rekaman CCTV sebagai barang bukti digital yaitu dalam kasus pembunuhan Brigadir Nofriansyah Yosua Hutabarat (Brigadir J) yang terjadi pada 8 Juli 2022, rekaman CCTV menunjukkan tanda-tanda manipulasi. Ahli forensik digital Abimanyu Wahyuwidayat menemukan bahwa dua mobil di garasi terlihat terkompres, format video tidak sesuai standar, dan penunjuk waktu (time stamp) sulit dibaca. Selain itu, intensitas cahaya berbeda saat Putri Candrawathi tiba dan kembali, menunjukkan kemungkinan pengeditan. Jeda waktu hanya 13 menit untuk mengganti pakaian juga mencurigakan, menandakan bahwa ada durasi yang hilang dalam rekaman. Temuan ini menekankan pentingnya bukti video dalam proses hukum (Saptohutomo, 2022).

Munculnya berbagai macam perangkat lunak pengeditan video membuat sulit bagi seseorang untuk membedakan antara video yang telah dimanipulasi dengan video asli (Johnston et al., 2020). Semua konten yang berhubungan dengan multimedia sangat mudah untuk diubah menggunakan beberapa perangkat lunak penyuntingan digital (Stamm et al., 2012). Perkembangan perangkat lunak pemrosesan gambar dan video seperti *Photoshop, Adobe Premiere*, *Final Cut Pro*, VN, dan lainnya yang memungkinkan manipulasi media visual digital dengan mudah tanpa meninggalkan jejak yang jelas (Jia et al., 2018). Perangkat tersebut memberikan dukungan yang hebat untuk mengedit video dengan mudah, dan siapa pun dapat mengedit video sesuai keinginannya (Nguyen et al., 2020). Setiap orang dapat dengan mudah menggunakan perangkat lunak editing video untuk mengubah frame, menyusun ulang urutan kejadian, atau bahkan menambahkan elemen palsu ke dalam video.

Tujuan dari manipulasi ini bervariasi, termasuk untuk menghilangkan bukti kejahatan, menyebarkan informasi palsu, atau menciptakan naratif yang memihak kepada pihak tertentu. Para penjahat sering memanfaatkan kerentanan ini, sehingga proses investigasi menjadi semakin sulit dalam membedakan antara video asli dan yang telah dimanipulasi. Banyak pelaku kejahatan seringkali tidak dapat dipidanakan karena rekaman video yang menjadi bukti kejahatan tersebut tidak dapat digunakan karena telah dimanipulasi (Pandey et al., 2014). Video yang telah dimanipulasi dapat menyulitkan pihak polisi dalam memecahkan masalah dan juga sulit digunakan dalam keputusan pengadilan (Akhtar et al., 2024). Maka dari itu penting untuk dilakukan pemeriksaan integritas pada video saat digunakan sebagai barang bukti dalam sebuah kasus dipengadilan (Yu et al., 2016). Deteksi manipulasi video bertujuan untuk memastikan keaslian serta mengidentifikasi potensi modifikasi atau pemalsuan, guna memverifikasi apakah video tersebut asli atau tidak (Akhtar et al., 2022). Keputusan mengenai keaslian pada video biasanya dibuat dengan

bantuan teknik-teknik tertentu, yang secara kolektif disebut sebagai teknik deteksi pemalsuan (Kingra et al., 2017).

Salah satu jenis pengeditan video yang dikenal sebagai *tampering* melibatkan penyisipan objek tertentu ke dalam suatu rekaman video. Objek yang disisipkan ini bisa berupa serangkaian frame dari video yang sama atau berbeda, potongan frame lain dari video yang sama atau berbeda, atau bahkan gambar yang dimasukkan ke dalam beberapa frame secara bersamaan (A. J. Justicia & Riadi, 2018). Maka dari itu forensik multimedia memiliki peran yang bertujuan untuk mengatasi kebutuhan ini dengan menyediakan algoritma dan sistem yang membantu penyelidik menemukan jejak manipulasi dan mengekstrak informasi tentang riwayat item multimedia (Zampoglou et al., 2019). Untuk menguji keaslian suatu video, terdapat dua klasifikasi metode yang umum digunakan, yaitu *tampering detectio*n dan *tampering localization*. *Tampering detection* adalah metode yang digunakan untuk mengidentifikasi apakah ada manipulasi dalam integritas video tanpa menunjukkan area yang spesifik yang telah dimanipulasi. Sementara itu, *tampering localization* adalah metode yang memfokuskan pada menunjukkan area tertentu dalam video yang telah mengalami manipulasi (Bestagini et al., 2013).

Penelitian tentang mendeteksi video *tampering* telah banyak dilakukan oleh peneliti sebelumnya, seperti yang dilakukan oleh (Yunita Sari et al., 2017) yang fokus pada analisis video forensik untuk identifikasi manipulasi pada video yang diambil dengan handycam, menggunakan metode *Localization Tampering*. Metode ini mencakup simulasi berbagai jenis manipulasi seperti pemotongan, zoom, rotasi, dan skala abu-abu. Namun penelitian ini memiliki kelemahan karena hanya terbatas pada analisis video dari handycam, tidak mencakup dari perangkat lain seperti CCTV atau smartphone, yang sering digunakan dalam kasus kejahatan saat ini. Selain itu, analisis meski dilakukan secara *frame by frame*, penelitian ini tidak menyentuh aspek lain yang penting seperti integritas data atau metadata. Penelitian lain juga dilakukakan oleh (A. P. Justicia & Riadi, 2018) membahas Analisis Video Forensik dalam Data Penyimpanan. Metode yang digunakan mencakup *zooming, Laplacian, Sharpening, Contrast brightness*, *optical deblurring, exposure, turbulence deblurring, Wiener filter, bilateral filter, unsharp masking*, dan *homomorphic filter*. Hasil penelitian menegaskan bahwa video asli dan video perusakan dapat diverifikasi keasliannya melalui serangkaian pengujian menggunakan teknik seperti *Optical Deblurring, Turbulence Deblurring, Contrast Brightness, Exposure, Laplacian Sharpening, Unsharp Masking, Wiener Filter, Bilateral Filter, Homomorphic Filter*, dan *Temperature Tint* dengan bantuan software AMPED FIVE Ultimate 9010. Penelitian ini menunjukkan bahwa 70% dari

rekaman dapat diidentifikasi dengan akurat menggunakan teknologi digital modern, seperti AMPED FIVE Ultimate 9010. Meskipun penelitian ini berhasil menunjukkan efektivitas identifikasi, ia kurang mendalam dalam metode *frame by frame* dan tidak menjelaskan bagaimana setiap frame dianalisis untuk mendeteksi manipulasi. Selain itu, penelitian ini tidak mengeksplorasi teknik lain, seperti perbandingan hash atau analisis kontras, yang dapat memperkuat keakuratan bukti video. Sementara itu, penelitian juga dilakukan oleh (Riadi et al., 2023) yang melakukan pengujian data video dengan menggunakan framework *Generic Computer Forensic Investigation Model* (GCFIM) untuk dapat memberikan informasi yang terstruktur dan valid untuk dapat diterima dalam persidangan sebagai barang bukti digital. Hasil pengujian menunjukkan perbedaan yang signifikan antara video asli dan video yang telah dimanipulasi, seperti perbedaan ukuran file, durasi video, dan tanggal. Kelemahan dari penelitian ini adalah fokus utamanya pada analisis metadata, yang mengabaikan analisis visual dan *frame by frame* yang dapat mengungkap manipulasi lebih mendalam. Selain itu, teknik lain seperti analisis hash atau pengujian kualitas video tidak dibahas, padahal informasi tersebut dapat memberikan gambaran lebih lengkap tentang keaslian dan keutuhan rekaman. Selain itu beberapa penelitian lainnya yang juga telah berusaha menangani permasalahan manipulasi video ini dengan mengembangkan metode untuk mendeteksi dan menganalisis perubahan yang terjadi pada video digital. Salah satu teknik yang sering digunakan adalah analisis metadata, yang mengidentifikasi perubahan dalam ukuran file, durasi, frame rate, dan aspek teknis lainnya untuk mendeteksi adanya manipulasi (Albanna & Riadi, 2017). Metode lain yang populer adalah analisis histogram dan *frame-by-frame comparison*, yang memanfaatkan perbedaan dalam distribusi warna atau kecerahan piksel untuk mengidentifikasi perubahan pada frame yang telah dimanipulasi (Pedapudi & Vadlamani, 2023).

Secara keseluruhan, meskipun masing-masing penelitian memberikan kontribusi penting dalam bidang analisis video forensik, namun juga memiliki keterbatasan dalam mencakup perangkat dan metode analisis yang digunakan. Dengan adanya beberapa penelitian yang sudah dilakukan yang membahas tentang mendeteksi keaslian video dengan berbagai metode yang berbeda. Penelitian ini bertujuan untuk mengatasi permasalahan mengenai manipulasi video yang terdapat dalam CCTV dengan menerapkan metode *Localization Tampering* yang memanfaatkan teknik frame by frame. Diharapkan bahwa metode ini dapat menjadi solusi yang efektif dalam memastikan keaslian rekaman video CCTV dan menghindari potensi kerugian yang dapat ditimbulkan akibat manipulasi video.

1.2 Rumusan Masalah

Adapun rumusan masalah yang terdapat dalam penelitian ini yaitu sebagai berikut:

a. Bagaimana implementasi metode *Localization Tampering* dalam melakukan deteksi rekayasa rekaman video cctv?
b. Bagaimana efektivitas dan akurasi metode *Localization Tampering* dalam melakukan deteksi rekayasa rekaman video cctv?

1.3 Tujuan Penelitian

Tujuan masalah dalam penelitian ini yaitu sebagai berikut:

a. Menerapkan metode *Localization Tampering* dalam konteks deteksi rekayasa rekaman video CCTV melaui algoritma yang dapat memeriksa keaslian setiap frame.
b. Mengetahui kapasitas dan akurasi metode *Localization Tampering* dalam melakukan deteksi rekayasa rekaman video cctv.

1.4 Manfaat Penelitian

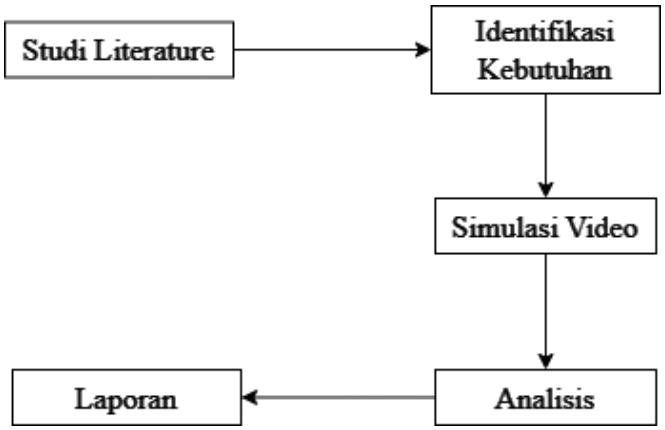
Manfaat dari penelitian ini adalah dapat membantu penyidik untuk mendeteksi manipulasi dalam video dengan menerapkan metode *localization tampering*. Penelitian ini juga dapat meningkatkan akurasi keaslian video dalam meningkatkan sistem keamanan, serta dapat dijadikan sebagai barang bukti yang sah dalam kasus persidangan.

1.5 Batasan Masalah

Batasan masalah dalam penelitian ini hanya berfokus pada analisis keaslian video pada rekaman CCTV yang sudah dilakukan serangan seperti *zooming, cropping, grayscale, delection, rotation,* dan *add frame* menggunakan metode *Localization Tampering*. Adapun aspek lain diluar dari analisis yang dilakukan tidak akan dibahas dalam penelitian ini.

1.6 Metode Penelitian

Adapun beberapa tahapan-tahapan yang dilakukan dalam proses penelitian yaitu sebagai berikut:



Gambar 1.1. Alur Metode Penelitian

Terdapat beberapa tahapan yang dilakukan dalam penelitian ini, diantaranya diawali dengan studi literatur, identifikasi kebutuhan, simulasi video, analisis, dan laporan.

a. Studi Literatur

Pada penelitian ini dilakukan tahapan studi literatur dengan mengeksplorasi karya-karya penelitian yang relevan dengan topik penelitian yang dijalankan. Tahapan ini dilakukan dengan mencari dan mengumpulkan teori atau referensi dari sumber akademis seperti jurnal ilmiah, paper, buku, dan artikel yang relevan dengan topik penelitian yang dijalankan.

b. Identifikasi Kebutuhan

Dalam penelitian ini dilakukan tahapan identifikasi kebutuhan dengan menyiapkan alat dan bahan untuk keperluan analisis.

c. Simulasi Video

Pada tahapan simulasi video ini dilakukan penggandaan file video yang didapat dari rekaman CCTV. File video dari hasil *copy* kemudian dilakukan tampering atau serangan yang berupa *zooming, cropping, grayscale, delection, rotation,* dan *add frame* untuk menghasilkan video yang berbeda dari video asli.

d. Analisis

Tahapan analisis dalam penelitian ini diterapkan metode *Localization Tampering.* Metode ini dilakukan untuk mendeteksi serangan yang ada dalam video.

e. Laporan

Pada tahapan ini dihasilkan laporan yang mencangkup ringkasan metode peneltian,

hasil, serta kesimpulan dari penelitian yang dilakukan.

1.7 Sistematika Penelitian

Penelitian ini menggunakan sistematika metodelogi peneltian atau kerangka penelitian yaitu sebagai berikut:

BAB I: Pendahuluan

Pendahuluan ini menjelaskan latar belakang pentingnya penelitian deteksi rekayasa video CCTV dalam konteks keamanan dan forensik digital. Diterangkan pula tujuan penelitian, identifikasi masalah keaslian rekaman, dan solusi perbaikan yang diusulkan untuk meningkatkan keamanan digital.

BAB II: Tinjauan Pustaka

Pada tinjauan pustaka ini mengkaji penelitian sebelumnya terkait deteksi tampering video, metode *Localization Tampering*, dan analisis keaslian video. Selain itu, dibahas konsep dasar tentang forensik digital, bukti digital, video forensik, CCTV, dan juga oenjelasan mengenai *Localization Tampering* untuk memperkuat pemahaman terhadap topik ini.

BAB III: Metodologi

Bab ini menjelaskan langkah-langkah penelitian yang digunakan untuk mendeteksi rekayasa video CCTV menggunakan metode *Localization Tampering*. Dijelaskan juga teknik yang digunakan, seperti analisis frame by frame, histogram, dan grafik histogram.

BAB IV: Hasil Dan Pembahasan

Pada bab ini memaparkan hasil analisis yang dilakukan, menunjukkan frame dan durasi video yang telah dimanipulasi, serta mengevaluasi efektivitas dan akurasi metode *Localization Tampering* yang diterapkan dalam penelitian ini. Pembahasan hasil mencakup interpretasi temuan dan relevansinya terhadap tujuan penelitian.

BAB V: Kesimpulan Dan Rekomendasi

Bab ini merangkum hasil penelitian dan menjawab rumusan masalah yang telah diidentifikasi. Diberikan pula rekomendasi untuk memperbaiki metode deteksi rekayasa video CCTV yang telah diuji, serta saran bagi praktisi forensik digital untuk meningkatkan kesadaran dan kemampuan dalam mendeteksi manipulasi video, guna memastikan integritas bukti digital di masa mendatang.