

BAB II

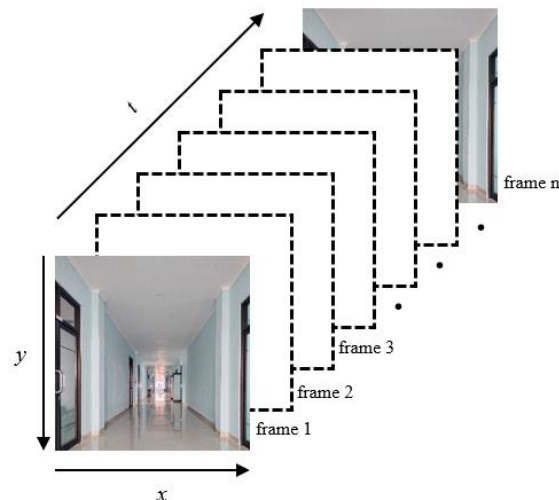
TINJAUAN PUSTAKA

2.1 Landasan Teori

2.1.1 Video

Video adalah elemen utama dalam konten multimedia yang memanfaatkan teknologi modern sebagai media penyampaian pesan, informasi, dan hiburan. Video menggabungkan aspek audio dan visual yang memiliki potensi menciptakan kesan yang lebih mendalam daripada media statis seperti gambar atau teks (Wardhani & Madenda, 2016). Dalam persidangan, pertanyaan terkait dengan barang bukti rekaman video berfokus pada keaslian video tersebut. Oleh karena itu dilakukan analisis metadata dan *frame* untuk memastikan keaslian rekaman video (Al-Azhar, 2012).

Secara visual, video terdiri dari rangkaian gambar atau *frame* bergerak yang dibaca berurutan dengan jumlah tertentu tiap detik yang menunjukkan tindakan berkesinambungan dalam urutan gambar (Widiarto, 2016). Umumnya, video direkam dengan kecepatan antara 25 hingga 30 *frame* per detik. Kecepatan tersebut disesuaikan dengan kecepatan alami pengamatan visual manusia dalam memahami urutan gambar yang ada dalam video (Madenda & Drajat, 2015). Video dapat direpresentasikan dalam tiga dimensi; dua dimensi spasial dan satu dimensi temporal (K & B.M, 2016). Seperti yang ditunjukkan pada Gambar 2.1.



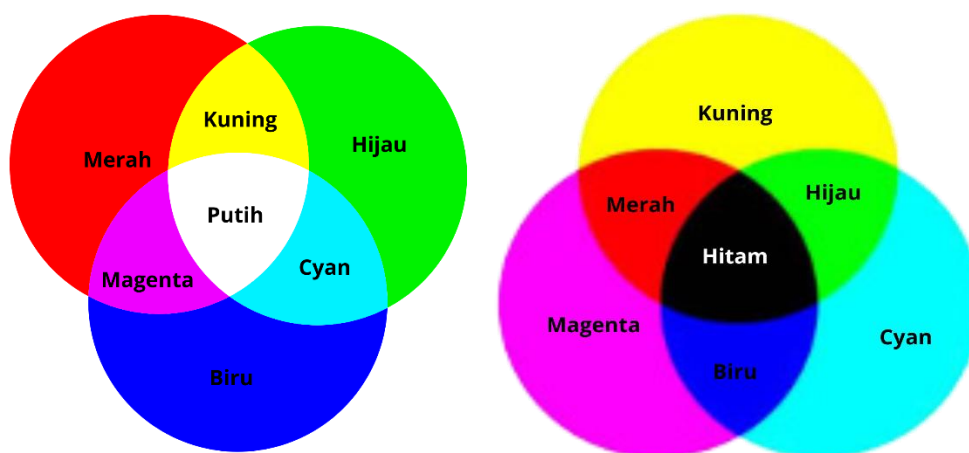
Gambar 2.1 Video sebagai rangkaian *frame* (Sumber: Sitara dan Mehtre, 2016)

Berdasarkan gambar 2.1, dimensi spasial merujuk pada panjang dan lebar setiap *frame*. Sementara itu, dimensi temporal mencakup urutan waktu dari *frame* tersebut. Video mengandung informasi *spatio temporal* yang mencakup aspek ruang (spasial) dan waktu (temporal). Aspek spasial mengacu pada informasi yang terkait dengan bentuk, posisi, dan struktur objek dalam *frame* video. Aspek temporal berkaitan dengan perubahan dan pergerakan objek di sepanjang rentang waktu dari awal hingga akhir video (Wardhani & Madenda, 2016).

2.1.2 Citra RGB

Model warna RGB adalah model warna yang didasarkan pada penambahan intensitas tiga cahaya primer, yaitu merah (*red*), hijau (*green*), dan biru (*blue*). Warna-warna dasar pada model RGB berfungsi sebagai acuan standar yang dapat ditampilkan secara universal dan diubah menjadi berbagai kode warna. Untuk meningkatkan efisiensi dalam proses deteksi, gambar RGB sering dikonversi menjadi gambar dalam format HSV. HSV sendiri merupakan representasi warna berbentuk silinder, sedangkan RGB menggunakan representasi dalam bentuk

koordinat kartesius. HSV adalah singkatan dari *Hue*, *Saturation*, dan *Value*. *Hue* menunjukkan tingkat kemurnian suatu warna terhadap warna aslinya, *Saturation* menggambarkan seberapa banyak warna putih yang terdapat dalam suatu citra, sementara *Value* menunjukkan tingkat kegelapan warna tertentu, sebagaimana ditunjukkan pada gambar 2.2 (Rif'ah & Arif, 2016).



Gambar 2.2 Model Warna Citra RGB (Sumber: Rif'ah & Arif, 2016)

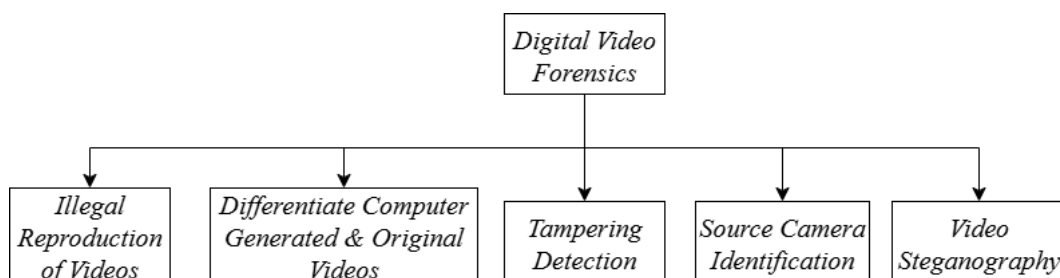
Berdasarkan Gambar 2.2, dapat dilihat perbandingan antara model warna RGB dan model warna HSV. Pada model warna RGB (bagian kiri), tiga warna primer yaitu merah, hijau, dan biru saling tumpang tindih menghasilkan warna-warna sekunder seperti kuning, cyan, dan magenta, serta menghasilkan warna putih pada area pertemuan ketiga warna primer tersebut. Sementara itu, pada model warna HSV (bagian kanan), pertemuan ketiga warna primer justru menghasilkan warna hitam, yang mencerminkan perbedaan mendasar dalam cara kedua model tersebut merepresentasikan warna. Perbedaan ini menunjukkan bahwa model RGB lebih berfokus pada emisi cahaya, sedangkan model HSV lebih merepresentasikan persepsi warna secara intuitif sesuai dengan cara pandang manusia terhadap warna (Rif'ah & Arif, 2016).

2.1.3 Digital Forensik

Digital forensik adalah salah satu cabang ilmu yang bertujuan untuk memperoleh informasi dan menyelidiki barang bukti digital agar bisa dipertanggungjawabkan di pengadilan sebagai barang bukti yang sah di mata hukum (Isnaini dkk., 2020). Proses dalam digital forensik secara umum terdiri atas kegiatan-kegiatan yaitu identifikasi atau administrasi penerimaan yang adalah pencatatan terhadap bukti-bukti yang akan diteliti seperti merek, model, serial. Akuisisi adalah kegiatan memisahkan harddisk untuk dilakukan imaging. Analisis adalah kegiatan menganalisis dengan cara menghubungkan keterkaitan jenis kejahatan dengan bukti-bukti, pelaporan adalah keseluruhan hasil kegiatan dalam bentuk tertulis (Army, 2020).

2.1.4 Forensik Video (*Video Forensics*)

Forensik video adalah suatu bidang ilmu yang berfokus pada analisis dan penyelidikan terhadap rekaman video untuk memverifikasi keaslian, integritas, dan keandalan informasi yang terkandung di dalamnya. Forensik video menitikberatkan penganalisan video melalui *frame by frame analysis* untuk memverifikasi keberadaan informasi atau hal-hal tertentu yang diduga akan mendukung atau menguatkan proses penyidikan (Al-Azhar, 2012).



Gambar 2.3 Klasifikasi Deteksi *Tampering* (Sumber: Sitara dan Mehtre, 2016)

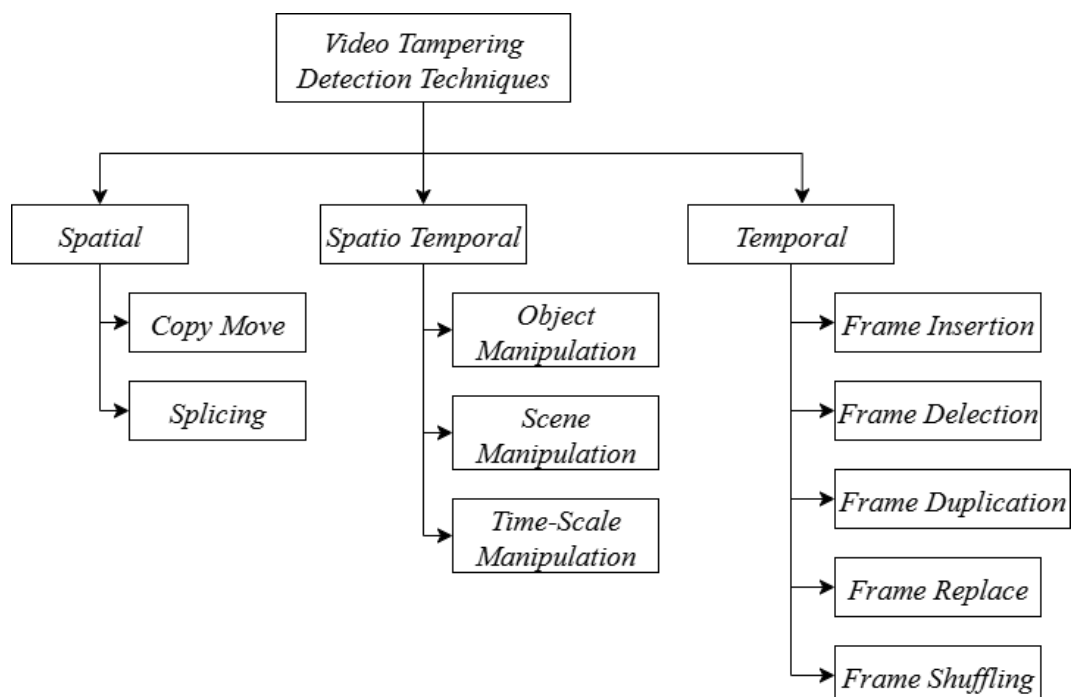
Klasifikasi forensik video digital ditunjukkan pada Gambar 2.3, yang terdiri dari lima kategori. Klasifikasi forensik video digital ditunjukkan pada Gambar 2.3, yang terdiri dari lima kategori. Pertama, identifikasi salinan video palsu untuk perlindungan hak cipta. Kedua, perbedaan antara video yang dihasilkan komputer dan video nyata. Ketiga, pendeteksian manipulasi video yang dapat didefinisikan sebagai pendeteksian modifikasi berbahaya dari konten video, yang dilakukan untuk menyembunyikan suatu objek, peristiwa atau mengubah makna video dalam urutan video. Keempat, identifikasi kamera sumber berkaitan dengan mengidentifikasi perangkat spesifik yang digunakan untuk merekam video yang sedang diperiksa. Kelima, steganografi video merupakan seni menyembunyikan informasi dalam media penutup, dimana steganalisis video berkaitan dengan pendeteksian informasi tersembunyi dalam file video (Sitara dan Mehtre, 2016).

2.1.5 Video Tampering

Video tampering adalah proses mengubah isi video dengan maksud untuk menyembunyikan suatu objek, peristiwa atau mengubah makna yang disampaikan oleh gambar dalam video (Sitara dan Mehtre, 2016). *Tampering* dan modifikasi citra memiliki keterkaitan karena keduanya melibatkan tindakan manipulasi atau mengubah citra. Meski demikian, terdapat perbedaan mendasar antara keduanya, yaitu terletak pada tujuan dari manipulasi tersebut. Mengubah citra dalam modifikasi citra memiliki tujuan yang lebih luas, termasuk peningkatan estetika, penyampaian pesan, atau penyembunyian informasi. Tindakan mengubah citra

pada *tampering* bertujuan untuk menyesatkan atau mengubah persepsi (Sari dkk., 2017).

Video tampering dapat dikategorikan menjadi tiga kelompok utama berdasarkan jenis perubahan yang dilakukan pada video, seperti yang disajikan pada Gambar 2.4.



Gambar 2.4 Klasifikasi teknik pendeteksian *video tampering* (Sumber: Sitara dan Mehtre, 2016)

Klasifikasi *tampering* pada video dikelompokkan menjadi tiga kategori yaitu sebagai berikut (Diwan dkk., 2024):

1. *Spatial*

Manipulasi spasial adalah bentuk modifikasi video yang melibatkan perubahan konten visual di dalam satu atau beberapa *frame* video, dimana perubahan tersebut dapat terjadi *pada* objek latar depan maupun objek latar belakang tanpa mengubah urutan atau durasi *frame* video tersebut. Manipulasi spasial dalam video memiliki tiga jenis serangan utama.

Pertama adalah penambahan objek (*object addition*), yang merupakan jenis manipulasi dimana objek ditambahkan ke dalam satu atau beberapa *frame* video. Contoh umum yang sering dijumpai adalah *copy-move tampering* atau *copy-paste*, dimana bagian tertentu dari *frame* video disalin dan ditempelkan di lokasi lain. Tujuan dari manipulasi ini adalah menambahkan informasi palsu atau menghilangkan informasi penting.

Kedua adalah penghapusan objek (*object removal*) yang dilakukan dengan menghapus atau menghilangkan objek dari *frame* video, baik pada latar depan maupun latar belakang. Dalam proses ini, teknik *inpainting* digunakan untuk merekonstruksi area yang telah dihapus atau rusak agar tetap terlihat alami.

Ketiga adalah modifikasi objek (*object modification*) yang melibatkan perubahan objek dalam *frame*. Modifikasi ini dapat dilakukan dengan mengubah ukuran, bentuk, warna, atau menerapkan berbagai efek untuk mengubah karakteristik objek.

Beberapa contoh teknik manipulasi yang termasuk kategori splicing diantaranya adalah *face swap*, yaitu penggantian wajah seseorang dalam video atau gambar dengan wajah orang lain, dan *superimposing* yang merupakan penempatan suatu objek diatas objek lain sehingga keduanya berada dalam satu lapisan yang sama atau tumpang tindih.

2. *Spatio-Temporal*

Manipulasi spatiotemporal terjadi ketika video dimanipulasi baik dalam *frame* maupun antar-*frame* secara bersamaan, yang membuatnya sulit untuk dideteksi. Ada tiga jenis utama manipulasi ini. Pertama, manipulasi objek, yang

melibatkan penghapusan atau penambahan objek dalam *frame* untuk mengubah konteks visual, mengubah alur cerita, atau menghilangkan bukti tertentu. Kedua, manipulasi adegan, yaitu pengaturan ulang urutan atau durasi adegan dalam video untuk mengganggu alur cerita dan menyesatkan penonton. Ketiga, manipulasi kecepatan waktu, yang dilakukan dengan mempercepat atau memperlambat bagian tertentu atau seluruh video untuk menonjolkan atau mengurangi kejadian, serta menciptakan efek dramatis.

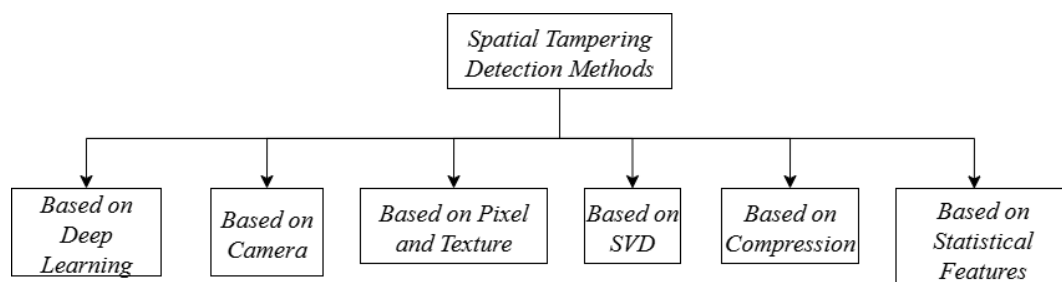
3. *Temporal*

Perubahan temporal mencakup lima teknik, yaitu *frame insertion*, *frame deletion*, *frame duplication*, *frame replacement*, dan *frame shuffling*. *Frame insertion* merupakan teknik manipulasi yang menyisipkan satu atau lebih *frame* ke dalam urutan video tanpa mengganti *frame* yang sudah ada. *Frame deletion* adalah teknik manipulasi yang menghapus *frame* tertentu dari urutan video yang mengakibatkan perubahan alur kejadian. *Frame duplication* merupakan teknik manipulasi dengan menambahkan salinan dari *frame* tertentu yang menciptakan pengulangan visual. *Frame replacement* adalah teknik manipulasi yang mengganti satu atau beberapa *frame* dengan *frame* dari video lain. *Frame shuffling* merupakan teknik manipulasi dengan mengacak urutan *frame* dalam video.

2.1.6 *Localization Tampering*

Localization Tampering adalah metode deteksi yang dapat mengidentifikasi bagian pada video yang telah dimanipulasi, dengan tujuan memberikan informasi terkait lokasi manipulasi dalam bentuk koordinat piksel spasial dan urutan *frame*

temporal di mana manipulasi terjadi (Bestagini dkk., 2013). Metode ini dapat dilakukan dengan berbagai pendekatan tergantung jenis *tampering* yang diterapkan. Untuk *attack* spasial, *Localization Tampering* dapat dilakukan dengan metode berdasarkan fitur piksel dan tekstur, metode berdasarkan SVD (*Singular Value Decomposition*), metode berdasarkan fitur kompresi, dan metode berdasarkan fitur statistik, seperti yang ditunjukkan pada gambar 2.5.



Gambar 2.5 Metode Deteksi *Spatial Tampering* (Sumber: Sitara dan Mehtre, 2016)

Salah satu pendekatan yang digunakan dalam *Localization Tampering* pada video adalah deteksi berbasis deteksi fitur piksel dengan perbedaan warna, yang berfokus pada analisis perubahan warna antar piksel dalam satu *frame* atau antar *frame*. Manipulasi spasial seperti penambahan, penghapusan, atau pengubahan objek dalam sebuah *frame* dapat menyebabkan ketidakkonsistenan warna yang terdeteksi melalui perbandingan nilai RGB atau YCbCr antar piksel. Ketidaksesuaian antara piksel di sekitar area manipulasi sering kali menjadi petunjuk adanya *tampering*. Pendekatan berbasis warna ini efektif dalam mendeteksi manipulasi, terutama jika manipulasi dilakukan tanpa memperhatikan konsistensi warna dengan area sekitarnya (Akhtar dkk., 2022).

2.1.7 Jarak Euclidean dan Centroid

Jarak Euclidean adalah metode perhitungan jarak antara dua titik dalam ruang berdimensi yang digunakan untuk mengukur kedekatan antar variabel (Pamungkas, 2019; Cahya dkk., 2023). Dalam pengolahan citra digital, jarak Euclidean memerlukan sebuah titik acuan tetap yang dikenal sebagai centroid. Dalam konteks pengolahan citra berbasis nilai warna, centroid merupakan titik tengah dari sekumpulan nilai data yang diperoleh dengan membagi nilai RGB setiap piksel dengan dua (Anggraini dan Prayudi, 2024).

Berikut rumus menghitung *centroid* pada persamaan (2.1) (Mualfah dkk., 2022):

$$C_{R,i} = \frac{R_i}{2}, \quad C_{G,i} = \frac{G_i}{2}, \quad C_{B,i} = \frac{B_i}{2} \quad (2.1)$$

Keterangan:

i = indeks *frame* ($i = 1, 2, \dots, N$)

N = jumlah *frame* yang dianalisis

R_i, G_i, B_i = nilai komponen merah, hijau, dan biru pada *frame* i

$C_{R,i}$ = centroid per *frame* untuk komponen R (merah) pada *frame* i

$C_{G,i}$ = centroid per *frame* untuk komponen G (hijau) pada *frame* i

$C_{B,i}$ = centroid per *frame* untuk komponen B (biru) pada *frame* i

Centroid yang telah ditetapkan kemudian digunakan sebagai titik acuan untuk mengukur jarak terhadap nilai RGB pada setiap *frame* yang sama menggunakan jarak Euclidean. Rumus yang digunakan dalam penghitungan ini ditunjukkan pada persamaan (2.2) berikut (Anggraini dan Prayudi, 2024):

$$F_i = \sqrt{(R_i - C_{R,i})^2 + (G_i - C_{G,i})^2 + (B_i - C_{B,i})^2} \quad (2.2)$$

Keterangan:

F_i = skor jarak (Euclidean) antara nilai RGB *frame* I dan centroid per *frame*-nya

R_i, G_i, B_i = nilai komponen merah, hijau, dan biru pada *frame* i

$C_{R,i}$ = centroid per *frame* untuk komponen R (merah) pada *frame* i

$C_{G,i}$ = centroid per *frame* untuk komponen G (hijau) pada *frame* i

$C_{B,i}$ = centroid per *frame* untuk komponen B (biru) pada *frame* i

Skor F dihitung secara terpisah untuk video asli dan video *tampering* pada setiap *frame* yang sama, sehingga menghasilkan nilai F asli dan nilai F *tampering* sebagai bahan pembandingan. Perbedaan nilai skor F mengindikasikan adanya manipulasi. Jika nilai skor F kedua video identik, maka *frame* dinyatakan tidak mengalami *tampering*. Sebaliknya, jika terdapat perbedaan nilai skor F, maka *frame* tersebut terindikasi telah dimanipulasi (Anggraini dan Prayudi, 2024).

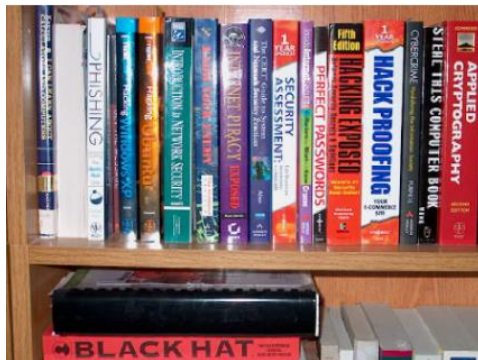
Kombinasi antara centroid sebagai titik acuan dan jarak Euclidean sebagai metode pengukuran memungkinkan sistem mendeteksi perubahan nilai warna antar *frame* secara kuantitatif dan akurat (Anggraini dan Prayudi, 2024).

2.1.8 Error Level Analysis (ELA)

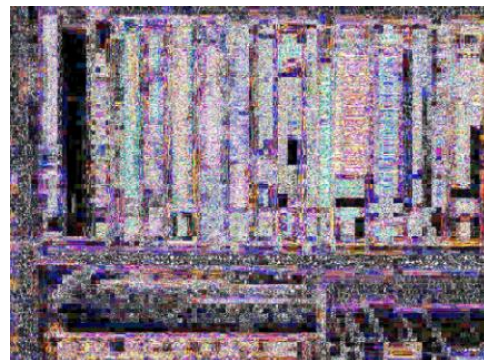
Error Level Analysis adalah metode untuk mengidentifikasi manipulasi citra dengan cara menyimpan ulang citra pada *level* kualitas tertentu, lalu mengkomputasi perbedaan antara citra kompresi dan citra sebelumnya. Metode ELA bekerja pada kisi-kisi gambar yang dikompresi secara independen dengan ukuran 8x8 piksel. Matriks dengan ukuran lebih besar dari 8x8 sulit untuk dimanipulasi secara matematis dan tidak didukung oleh perangkat keras, sedangkan

matriks dengan ukuran lebih kecil dari 8×8 tidak memiliki cukup informasi (Zhang dan Shi, 2021).

Metode ELA memiliki peran aktif dalam forensik gambar dan berguna dalam mendeteksi manipulasi pada gambar. Berikut contoh penggunaan ELA dalam mendeteksi manipulasi *splicing* pada gambar 2.6 (Krawetz, 2007).



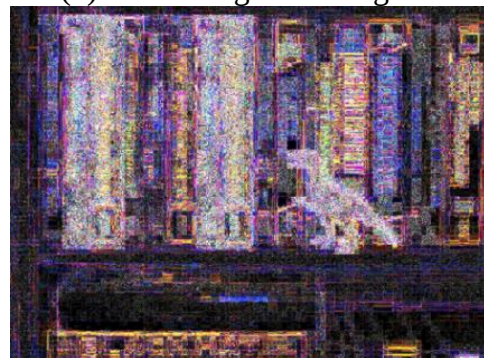
(a) Gambar original



(b) ELA dari gambar original



(c) Gambar manipulasi



(d) ELA dari gambar manipulasi

Gambar 2.6 Contoh Metode *Error Level Analysis* (Sumber: Krawetz, 2007)

Berdasarkan Gambar 2.6, dapat dilihat perbandingan hasil analisis menggunakan metode ELA pada gambar original dan gambar yang telah dimanipulasi. Gambar (a) menunjukkan gambar original berupa foto rak buku, sedangkan gambar (b) merupakan hasil ELA dari gambar original yang memperlihatkan pola *noise* yang relatif seragam dan merata di seluruh area gambar, mengindikasikan bahwa gambar tersebut belum mengalami manipulasi. Gambar (c) menunjukkan gambar yang telah mengalami manipulasi *splicing*, di mana terdapat

objek yang disisipkan ke dalam gambar original. Pada gambar (d) yang merupakan hasil ELA dari gambar manipulasi, terlihat adanya perbedaan tingkat kecerahan yang mencolok pada area yang telah dimanipulasi dibandingkan area sekitarnya. Perbedaan ini terjadi karena area yang dimanipulasi memiliki tingkat kesalahan kompresi yang berbeda, sehingga metode ELA berhasil mengidentifikasi dan memvisualisasikan lokasi manipulasi tersebut (Krawetz, 2007).

2.1.9 Tools yang digunakan dalam penelitian

Penelitian ini memanfaatkan beberapa tools dan perangkat lunak, yaitu *Python*, *Matlab*, *Forensically Beta*, dan *Capcut*.

1. *Python* merupakan bahasa pemrograman tingkat tinggi berorientasi objek (Bogdanchikov dkk., 2013). Dalam ekosistem *Python*, terdapat beberapa Pustaka yang digunakan dalam penelitian ini:
 - a. *OpenCV* adalah pustaka *open-source* yang digunakan untuk pengolahan citra, visi komputer, dan pembelajaran mesin. Fungsi utamanya meliputi membaca dan menulis gambar/video, deteksi objek dan fitur, peningkatan gambar, serta penyaringan (Parveen dan Shah, 2021).
 - b. *NumPy (Numerical Python)* adalah pustaka penting untuk komputasi numerik yang memungkinkan pemrosesan data dalam jumlah besar dengan kecepatan tinggi (Klemp, 2024).
 - c. *Pandas* adalah pustaka *Python* yang digunakan untuk manipulasi dan analisis data dari berbagai sumber seperti file *CSV*, *Excel*, dan *database SQL* (Pannadhitthana, 2025).

2. *Matlab (Matrix Laboratory)*, adalah perangkat lunak yang digunakan untuk pengolahan data dan analisis numerik (Atina, 2019).
3. *Forensically Beta*, adalah *tools* forensik gambar digital berbasis web untuk memeriksa keaslian dan potensi manipulasi pada gambar (Wagner, 2015).
4. *CapCut* adalah aplikasi pengeditan video dengan fitur menambahkan/memotong klip, menambahkan musik, stiker, dan filter artistik (Ispratiwi & Mellisa, 2023).

2.2 Penelitian Terkait (*State of The Art*)

Berdasarkan studi literatur tentang analisis manipulasi pada citra video dan citra gambar yang telah dilakukan sebelumnya yang memiliki fokus penelitian sejenis dengan penelitian yang akan dilakukan, maka didapat beberapa penelitian yang dikelompokkan pada Tabel 2.1.

Tabel 2.1 Penelitian Terkait (*State of The Art*)

No.	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
1.	Analisis Penerapan Metode <i>Exif Metadata</i> dan Metode <i>Error Level Analysis</i> untuk Pengolahan Forensik Digital	(Jaya Syafar dkk., 2025)	Metode <i>Exif Metadata</i> dan <i>Error Level Analysis</i> (ELA)	Hasil penelitian menunjukkan bahwa <i>Exif Metadata</i> hanya mendeteksi perbedaan metadata, seperti tanggal, waktu, atau pengaturan kamera, sedangkan <i>Error Level Analysis</i> (ELA) mendeteksi perubahan visual pada gambar. Penggabungan keduanya lebih efektif untuk mengidentifikasi manipulasi yang tidak terdeteksi metode tunggal.
2.	<i>Techniques for Video Authenticity Analysis Using the Localization Tampering Method to Support Forensic CCTV Investigations</i>	(Anggraini dan Prayudi, 2024)	Metode <i>Localization Tampering</i>	Hasil penelitian menunjukkan bahwa metode <i>Localization Tampering</i> mampu mengidentifikasi lokasi dan durasi manipulasi pada <i>frame</i> tertentu melalui analisis <i>frame</i> dan perbandingan histogram antara video asli dan video manipulasi. Metode ini berhasil mendeteksi berbagai bentuk manipulasi, seperti <i>zooming</i> , <i>cropping</i> , <i>grayscale</i> , penghapusan <i>frame</i> , dan rotasi, sehingga efektif mendukung investigasi forensik pada rekaman CCTV.
3.	Implementasi Metode <i>National Institute of Standards and Technology</i> (NIST) dalam Analisis Forensik untuk Mendeteksi	(ZH dkk., 2024)	Metode <i>National Institute of Standards and Technology</i> (NIST) dan Metode <i>Error</i>	Hasil penelitian menunjukkan bahwa citra asli dan manipulasi dapat dibedakan melalui metadata dan <i>Error Level Analysis</i> (ELA). Citra manipulasi menunjukkan perbedaan pola bintik, warna lebih gelap,

Tabel 2.1 Penelitian Terkait (*State of The Art*) (Lanjutan 1)

No.	Judul	Penulis dan Tahun	Metode	Hasil Penelitian
	Keaslian Citra Digital		<i>Level Analysis</i> (ELA)	serta adanya jejak <i>software editing Adobe Photoshop</i> pada metadata. Penggabungan <i>framework NIST</i> dan ELA terbukti efektif dalam mendeteksi keaslian citra digital.
4.	Forensik Citra Digital Menggunakan Metode <i>Error Level Analysis</i> , <i>Clone Detection</i> dan <i>Exif</i> Untuk Deteksi Keaslian Gambar	(Bisri & Marzuki, 2023)	Metode <i>Error Level Analysis</i> (ELA), Metode <i>Clone Detection</i> (CD), Metode <i>Exchangeable Image File</i> (EXIF)	Hasil penelitian menunjukkan bahwa metode <i>Error Level Analysis</i> , <i>Clone Detection</i> , dan <i>Exif Metadata</i> efektif dalam mendeteksi keaslian citra digital. <i>Error Level Analysis</i> memperoleh tingkat keberhasilan 94,6%, <i>Clone Detection</i> 94%, dan <i>Exif Metadata</i> 98,3% dalam mengidentifikasi citra digital yang telah dimanipulasi.
5.	Analisis Digital Forensik Keaslian Video CCTV Menggunakan Metode <i>Localization Tampering</i>	(Mualfah dkk., 2022a)	Metode <i>Localization Tampering</i>	Hasil penelitian menunjukkan bahwa metode <i>Localization Tampering</i> mampu mendeteksi manipulasi pada video CCTV berdurasi 1 menit, khususnya pada <i>frame</i> 6 hingga <i>frame</i> 33. Manipulasi berupa <i>attack frame</i> addition dan <i>attack frame</i> deletion teridentifikasi melalui analisis metadata, <i>frame</i> , histogram, serta perhitungan nilai RGB menggunakan <i>clustering K-Means</i> . Perbedaan grafik histogram dan jarak titik pusat <i>cluster</i> RGB membuktikan adanya <i>tampering</i> pada <i>frame</i> tersebut.

2.3 Matriks Penelitian

Matriks penelitian berisi pengelompokkan inti isi dari penelitian yang ada, diperuntukan sebagai pembandingan penelitian terdahulu dan penelitian yang akan dilakukan. Tabel 2.2 menggambarkan perbedaan penelitian yang diusulkan dengan penelitian terkait.

Tabel 2.2 Matriks Penelitian

No.	Penulis dan Tahun	Metode Analisis Manipulasi Gambar				
		<i>Localization Tampering</i>	<i>Error Level Analysis</i>	<i>Histogram Analysis</i>	<i>Clone Detection</i>	<i>Meta data</i>
1.	(Jaya Syafar dkk., 2025)		✓			✓
2.	(Anggraini dan Prayudi, 2024)	✓		✓		
3.	(ZH dkk., 2024)		✓			✓
4.	(Bisri & Marzuki, 2023)		✓		✓	✓
5.	(Mualfah dkk., 2022a)	✓		✓		✓
6.	Penelitian yang sedang dilakukan	✓	✓			

Berdasarkan tabel 2.2, penelitian yang paling relevan dengan penelitian ini adalah penelitian yang dilakukan oleh Anggraini dan Prayudi tahun 2024. Penelitian Anggraini dan Prayudi ini menerapkan metode *Localization Tampering* sebagai metode utama untuk mendeteksi manipulasi pada video CCTV, dengan analisis histogram sebagai metode validasi hasil. Namun penelitian tersebut belum menunjukkan secara spesifik area manipulasi yang terdapat pada *frame* (Anggraini dan Prayudi, 2024).

Gap penelitian muncul karena meskipun sama-sama menggunakan metode *Localization Tampering*, penelitian sebelumnya belum melanjutkan tahap analisis hingga mengungkapkan secara spesifik area pada gambar yang term manipulasi.

Penelitian ini mengisi kesenjangan tersebut dengan menambahkan tahapan menggunakan ELA sebagai analisis lanjutan setelah *frame* yang terindikasi manipulasi ditemukan, sehingga dapat memperkuat bukti dengan menampilkan visualisasi area spesifik yang telah dimanipulasi. Demikian penelitian ini diusulkan agar menghasilkan proses deteksi yang bukan hanya mampu mengidentifikasi keberadaan manipulasi pada tingkat *frame*, tetapi juga memberikan gambaran visual terhadap area perubahan yang terjadi.