Evaluasi Ketahanan *Hybrid Visible Watermarking* Berbasis Python terhadap Serangan Digital pada Video

Arip Padillah[1], Devi Mandiri[2], Muhammad Ridho Ramadhan[3], Muhammad Yusuf Firmansyah[4], Yunita[5]
[1,2,3,4,5] Program Studi Teknologi Informasi, Fakultas Teknik Informatika, Universitas Bina Sarana Informatika
Jl. RS. Fatmawati Raya No.24, Pd. Labu, Daerah Khusus Ibukota Jakarta
E-mail: 17220804@bsi.ac.id[1], 17221017@bsi.ac.id[2], 17210906@bsi.ac.id[3], 17221043@bsi.ac.id[4], yunita.ynt@bsi.ac.id[5]

***Abstract*—The widespread distribution of digital video content demands persistent copyright protection; however, static *visible watermarking* methods remain vulnerable to geometric manipulation. Moreover, quantitative evaluations of *visible watermarking* robustness on video content implemented in modern programming environments remain limited and are predominantly focused on static media. This study aims to evaluate the robustness of a hybrid *visible watermarking* system for video content through an experimental approach. The proposed system integrates spatial-domain processing, frequency-domain transformation based on the *Discrete Cosine Transform*, and multiscale techniques implemented using *Python* and *OpenCV*. Digital attack simulations include compression, format conversion, *resizing*, *noise*, and *cropping*, with performance assessed using *SSIM*, *pHash*, *MSE*, and histogram analysis. Experimental results demonstrate strong robustness against administrative attacks, maintaining *SSIM* values above 0.91 and *pHash* exceeding 0.97 under *H.264* compression and format conversion. Nevertheless, a *Robustness Paradox* is identified under *cropping* attacks, where trimming 12.5 percent on each side causes complete watermark detection failure, indicated by a *WM Area MSE* increase to 2,304.23, while color fidelity remains high with a histogram similarity value of 0.93. This study provides technical contributions in the form of empirical evidence on the limitations of static watermark placement and demonstrates that hybrid approaches offer a more balanced trade-off between visual quality and robustness, while recommending *dynamic watermarking* or advanced frequency-domain methods to improve resilience against geometric desynchronization.**

***Abstrak*—Distribusi konten video digital menuntut perlindungan hak cipta yang persisten; namun metode *visible watermarking* statis masih rentan terhadap manipulasi geometri. Selain itu, evaluasi kuantitatif terhadap ketahanan *visible watermarking* pada media video berbasis lingkungan pemrograman modern masih terbatas dan umumnya berfokus pada media statis. Penelitian ini bertujuan untuk mengevaluasi ketahanan sistem *visible watermarking* hibrida pada konten video menggunakan pendekatan eksperimental. Sistem yang diusulkan mengintegrasikan domain spasial, transformasi frekuensi berbasis *Discrete Cosine Transform*, serta pendekatan multiskala dengan implementasi *Python* dan *OpenCV*. Simulasi serangan digital meliputi kompresi, konversi format, *resizing*, *noise*, dan *cropping*, dengan evaluasi menggunakan metrik *SSIM*, *pHash*, *MSE*, dan analisis histogram. Hasil eksperimen menunjukkan ketahanan tinggi terhadap serangan administratif dengan nilai *SSIM* di atas 0,91 dan *pHash* melampaui 0,97 pada kompresi *H.264* dan konversi format. Namun demikian, fenomena *Robustness Paradox* teridentifikasi pada serangan *cropping*, di mana pemotongan area sebesar 12,5 persen pada setiap sisi menyebabkan kegagalan deteksi total dengan lonjakan *WM Area MSE* hingga 2.304,23, meskipun kesamaan histogram warna tetap tinggi dengan nilai 0,93. Penelitian ini memberikan kontribusi teknis berupa bukti empiris keterbatasan watermark statis dan menunjukkan bahwa pendekatan hibrida lebih efektif dalam menyeimbangkan kualitas visual dan ketahanan, sekaligus merekomendasikan *dynamic watermarking* atau metode domain frekuensi lanjut untuk meningkatkan ketahanan terhadap desinkronisasi geometris.**

***Kata Kunci*—Hak Cipta, Ketahanan Video, OpenCV, Python, Serangan Digital, *Visible Watermarking*.**

I. PENDAHULUAN

Era transformasi digital telah mendorong produksi dan konsumsi konten video secara masif melalui platform seperti YouTube dan media sosial lainnya. Namun, kemudahan distribusi ini diiringi oleh peningkatan ancaman pembajakan digital dan redistribusi ilegal yang merugikan pemilik hak cipta [1]. Meskipun instrumen hukum seperti UU No. 28 Tahun 2014 tentang Hak Cipta di Indonesia telah mengatur perlindungan karya, penegakan hukum secara regulatif dianggap belum memadai tanpa dukungan proteksi teknis yang proaktif [2]. Guna menghadapi tantangan tersebut, diperlukan upaya penanggulangan yang efektif melalui solusi teknologi multimedia. Selain penegakan hukum yang represif, salah satu solusi teknis yang paling banyak diimplementasikan dalam pengolahan citra digital adalah *watermarking* atau penandaan air [3].

Watermarking merupakan teknik yang umum digunakan untuk menandai kepemilikan dan hak cipta suatu citra, baik melalui tanda yang terlihat maupun melalui modifikasi pada level piksel atau kode *byte* yang tersembunyi [4]. Dalam literatur multimedia, teknik ini diklasifikasikan berdasarkan aspek kenampakannya menjadi dua kategori utama, yaitu *invisible* dan *visible watermarking* [5]. Secara spesifik, *invisible watermarking* memiliki sifat tidak dapat dideteksi oleh indra penglihatan manusia dan bertujuan menyisipkan informasi rahasia untuk melindungi hak cipta. Keberadaannya hanya dapat dideteksi melalui proses komputasi khusus untuk mengekstrak data yang telah disisipi [6]. Banyak riset berfokus pada domain frekuensi seperti *Discrete Cosine Transform* (DCT), *Discrete Wavelet*

Transform (DWT), atau *Discrete Fourier Transform* (DFT) karena ketahanannya yang tinggi [6],[7]. Namun demikian, *invisible watermarking* konvensional belum sepenuhnya tangguh terhadap serangan *analog hole* seperti *screen capture*. Distorsi berat yang dihasilkan oleh proses *screen capture* menyebabkan banyak skema *invisible watermarking* kehilangan ketahanan, sehingga *watermark* yang disisipkan cenderung rusak atau gagal diekstraksi [8].Sebaliknya, metode *visible watermarking* menimpakan suatu tanda yang berfungsi sebagai penanda kepemilikan visual yang eksplisit [9]. Penerapan *visible watermarking* tradisional sering dilakukan pada domain spasial karena beban komputasinya rendah dan efisien untuk aplikasi *real-time*. Namun, efisiensi ini sering kali mengorbankan ketahanan terhadap serangan manipulasi sinyal, tanda air pada domain spasial murni cenderung lebih rentan rusak akibat kompresi maupun operasi geometris seperti *cropping* dan *scaling* dibandingkan metode domain frekuensi yang secara inheren lebih protektif [10]**.**

Permasalahan yang menjadi celah penelitian saat ini adalah minimnya evaluasi kuantitatif terhadap ketahanan *robustness visible watermarking* yang diimplementasikan pada lingkungan pemrograman modern seperti Python. Banyak studi sebelumnya hanya berfokus pada keberhasilan penyisipan logo tanpa menguji secara mendalam seberapa kuat watermark tersebut bertahan terhadap degradasi sinyal yang umum terjadi di platform digital. Penelitian oleh Saifudin dan Widrani pada tahun 2021 berjudul "Rancang Bangun Sistem Digitalisasi Dokumen Menggunakan Metode Visible Watermark di Kantor Urusan Agama (KUA) Kecamatan Sayung″ terbatas pada penyisipan tanda air statis untuk dokumen arsip [9]. Demikian pula penelitian Gimnastiara et al. pada tahun 2025 berjudul "Implementasi Watermarking Pada Gambar Menggunakan Matlab Untuk Mencegah Plagiarisme Laporan Praktikum″ yang hanya memanfaatkan manipulasi teks sederhana pada citra diam [11]. Berbeda dengan studi-studi tersebut yang terbatas pada media statis, penelitian ini mengisi celah pada ranah video yang memiliki dinamika temporal. Kebaruan penelitian ini terletak pada penggunaan skema watermark hibrida yang menggabungkan *spatial-domain blending,* teknik multiskala*,* dan penguatan koefisien *Discrete Cosine Transform* (DCT) guna meningkatkan *robustness* terhadap berbagai manipulasi digital.

Penelitian ini bertujuan untuk mengevaluasi kinerja ketahanan teknik *Hybrid Visible Watermarking* berbasis Python melalui analisis eksperimental menggunakan metrik pHash (*Perceptual Hash*), SSIM (*Structural Similarity Index*), *MSE* (*Mean Squared Error*), dan analisis Histogram. Kontribusi utama penelitian ini adalah menyajikan data empiris mengenai efektivitas skema hibrida dalam menyeimbangkan kualitas visual dan perlindungan hak cipta konten video.

II. METODE PENELITIAN

A. Pendekatan Penelitian

Penelitian ini mengadopsi pendekatan eksperimental kuantitatif, sebuah metodologi yang berlandaskan pandangan *post-positivist* dan sistematis untuk menguji hubungan sebab-akibat antar variable [12]. Desain penelitian ini berfokus pada manipulasi variabel independen seperti implementasi teknik *visible watermarking,* dan pengukuran performa variabel yang objektif melalui pengumpulan data numerik, guna mengevaluasi efektivitas metode tersebut dalam kondisi yang terkendali [12]. Sesuai dengan karakteristik penelitin kuantitatif, data yang diperoleh akan dianalisis secara statistik untuk menguji hipotesis dan memastikan objektivitas serta keandalan hasil penelitian.

B. Tahapan Penelitian

Guna memastikan penelitian berjalan sistematis dan terstruktur, metodologi dibagi menjadi lima tahapan utama. Gambar 1 menunjukkan diagram alur penelitian yang mencakup seluruh rangkaian proses, mulai dari persiapan dataset hingga penarikan kesimpulan akhir.

Gambar 1. Alur Penelitian

Proses pada Gambar 1 diawali dengan pengumpulan dataset video, dilanjutkan dengan penyisipan watermark menggunakan algoritma hibrida yang diusulkan. Video yang telah disisipi watermark kemudian diuji ketahanannya melalui simulasi serangan digital. Hasil dari video yang diserang dievaluasi menggunakan metrik citra digital untuk dianalisis datanya guna mendapatkan kesimpulan mengenai efektivitas sistem.

C. Perangkat Penelitian

Guna menjamin replikasi penelitian, eksperimen dijalankan menggunakan perangkat keras dan lingkungan perangkat lunak dengan rincian spesifikasi teknis :

1. Perangkat Keras

   Eksperimen dijalankan pada laptop Apple dengan M2 Chip (8-core CPU, 8-core GPU) dan RAM

sebesar 16 GB. Arsitektur ini dipilih karena efisiensi pemrosesan instruksi multimedia berbasis ARM.

2. Sistem Operasi

   MacOS Tahoe 26.1.

3. Perangkat Lunak

   Sistem dikembangkan menggunakan bahasa pemrograman Python versi 3.14.0 Pustaka utama yang digunakan meliputi OpenCV (*cv2*) versi 4.12.0 untuk manipulasi matriks citra, NumPy untuk komputasi numerik, dan FFmpeg untuk manajemen *stream* audio-video serta proses *remuxing*.

D. Persiapan Dataset

Penelitian ini menggunakan sepuluh sampel video sebagai dataset uji. Penggunaan sepuluh sampel dianggap cukup representatif dalam konteks pengolahan sinyal digital karena fokus utama penelitian terletak pada pengujian integritas struktur piksel dan ketahanan algoritma terhadap manipulasi matematis, bukan pada analisis konten semantik secara luas. Sampel dipilih secara *purposive* untuk mewakili variasi karakteristik visual, yang mencakup orientasi video *landscape* (16:9) dan *portrait* (9:16), kompleksitas latar belakang dari polos hingga tekstur kompleks dengan pergerakan objek, serta penyiapan 2 logo watermark yang memiliki karakter dan warna berbeda dalam format PNG.

E. Implementasi Sistem Watermarking

Sistem dirancang untuk menyisipkan *visible watermark* hibrida yang bekerja pada domain spasial dan frekuensi secara simultan. Algoritma memproses video input secara *frame-by-frame*, kemudian membangun representasi multiskala menggunakan *Gaussian Pyramid* untuk mendistribusikan watermark pada berbagai tingkat resolusi. Pada setiap level, diterapkan operasi *hybrid overlay* yang mengombinasikan teknik *Alpha Blending* pada saluran luminans (Y) serta penguatan koefisien frekuensi melalui transformasi *Discrete Cosine Transform* (DCT).

Penelitian ini menetapkan posisi watermark di Pojok Kanan Atas dengan dua justifikasi teknis utama. Pertama, kepatuhan EBU R95, di mana posisi ini berada dalam *Safe Title Area* sesuai standar *European Broadcasting Union* guna memastikan logo tidak terpotong pada berbagai jenis layar monitor. Kedua, penghindaran *subtitle*, karena area bawah video sering digunakan untuk menampilkan takarir (*subtitle*) atau *closed caption*. Penempatan di kanan atas meminimalisir oklusi atau tumpang tindih antara teks informasi dengan tanda kepemilikan.

F. Parameter Teknis Serangan

Guna menguji ketahanan atau *robustness*, video master diuji dengan skenario serangan yang mensimulasikan gangguan transmisi dan manipulasi ilegal. Parameter serangan ditentukan berdasarkan standar distribusi konten digital saat ini melalui lima kategori utama:

1. *Compress*
   Kompresi merupakan suatu bentuk manipulasi dengan tujuan untuk memperkecil ukuran dari suatu file dengan tetap mempertahankan data didalamnya [13].
2. *Cropping*
   Cropping atau pemotongan merupakan tindakan menghilangkan sebagian area tepi video dengan batas tertentu [14].
3. *Noise*
   Noise adalah gangguan sinyal yang menyebabkan variasi acak pada kecerahan atau warna piksel, yang dapat menurunkan kualitas ataupun mutu dari suatu citra dan sering dianggap sebagai cacat citra [15].
4. *Convert*
   Convert atau konversi dalam bidang teknologi digambarkan secara umum dengan merubah suatu bentuk data ke bentuk lainnya dengan tetap mempertahankan informasi aslinya [16].
5. *Resize*
   Resize atau mengubah ukuran bertujuan agar citra berubah resolusinya baik *downscaling* ataupun *upscaling*, bisa secara vertikal ataupun horizontal [17].

Seluruh spesifikasi parameter yang diterapkan dalam simulasi serangan tersebut dirangkum secara mendetail dalam Tabel 1.

Tabel 1. Spesifikasi Parameter Simulasi Serangan

Kategori Serangan	Jenis Serangan	Parameter Teknis	Deskripsi Eksperimen
Kompresi Video	Low Compression	Codec H.264, CRF: 32	Penurunan kualitas standar distribusi web.
	Lowest Compression	Codec H.264, CRF: 40	Simulasi kompresi ekstrem pada bandwidth rendah.
Transformasi Geometri	Cropping	12.5% pada tiap sisi	Penghilangan area tepi secara simetris untuk membuang koordinat watermark.
	Resizing	1280 x 720 (Landscape) 720 x 1280 (Portrait)	Downscaling ke resolusi HD menggunakan interpolasi bicubic.
Manipulasi Sinyal	Noise	Jenis: Gaussian, Intensitas sigma = 0.5	Penambahan gangguan acak pada seluruh piksel frame.
Konversi Format	AVI (MPEG-4)	Codec: mpeg4, -qscale:v: 5	Konversi ke format warisan
	MKV (H.264)	Codec: libx264, CRF: 23	Transcoding ke kontainer Matroska.
	WebM (VP9)	Codec: libvpx-vp9, CRF: 30	Konversi ke format video berbasis web.
	MP4 (H.265/HEVC)	Codec: libx265, CRF: 28	Pengujian pada standar kompresi efisiensi tinggi terbaru.

G. Metrik Evaluasi

Pemilihan metrik evaluasi didasarkan pada kebutuhan analisis dari berbagai sudut pandang kualitas citra digital:

1. *Perceptual Hash* (pHash)
   Perceptual Hash dipilih karena kemampuannya untuk mendeteksi tingkat kesamaan suatu citra atau gambar [18]. pHash efektif mendeteksi kemiripan

fitur visual secara global meskipun piksel telah dimodifikasi secara minor.

2. *Structural Similarity Index* (SSIM)
   SSIM dipilih karena dapat digunakan untuk membandingkan antara 1 citra dengan citra lainnya [19]. SSIM merupakan metrik yang mengukur degradasi kualitas gambar berdasarkan tiga komponen utama yaitu luminans, kontras, dan struktur.
3. *Mean Squared Error* (MSE)
   Mean Squared Error (MSE) digunakan untuk mengukur rata-rata selisih kuadrat antara piksel-piksel pada citra asli dan citra yang diproses oleh serangan manipulasi [20].
4. Histogram
   Digunakan untuk menganalisis dan membandingkan distribusi intensitas warna pada ruang warna HSV antar *frame* [21]. Metrik ini berguna untuk mendeteksi perubahan drastis pada karakteristik warna akibat kompresi atau penerapan filter pada citra.

Validasi internal dilakukan dengan memastikan bahwa setiap proses penempelan watermark dan simulasi serangan dijalankan secara otomatis melalui skrip Python yang sama untuk seluruh sampel, guna menghilangkan bias manual dan menjamin konsistensi data hasil eksperimen.

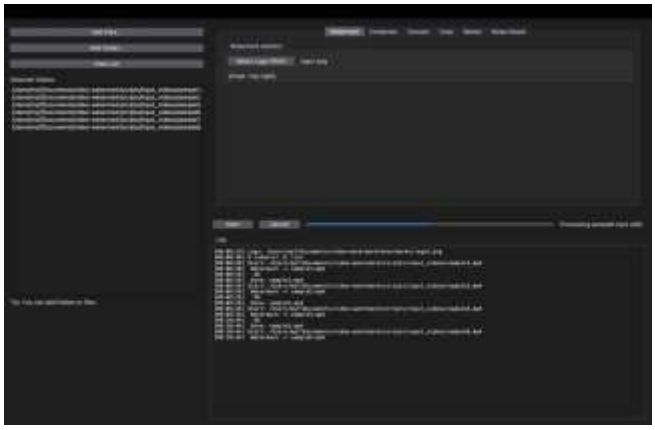
H. Analisis Hasil

Data kuantitatif yang diperoleh dari seluruh metrik dikompilasi ke dalam format terstruktur seperti csv dan xlsx. Tahap analisis bertujuan untuk mengukur tingkat kerusakan visual yang ditimbulkan oleh setiap jenis serangan, menentukan metrik yang paling sensitif terhadap jenis serangan tertentu, serta menilai apakah watermark masih dapat terdeteksi secara objektif setelah simulasi serangan terjadi. Analisis ini menjadi dasar penarikan kesimpulan mengenai efektivitas metode *visible watermarking* hibrida sebagai solusi perlindungan hak cipta digital pada media video.

III. HASIL DAN PEMBAHASAN

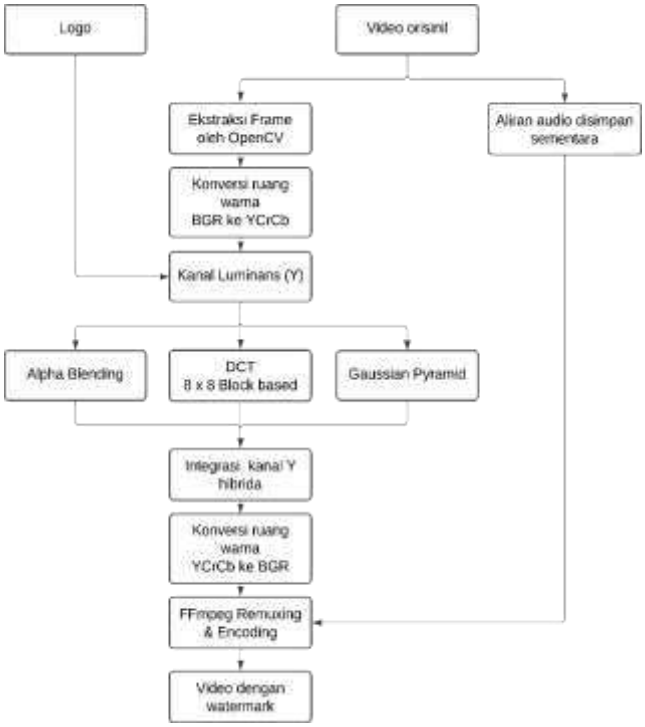
A. Implementasi Sistem Watermarking Hibrida

Sistem *visible watermarking* yang dirancang dalam penelitian ini mengadopsi arsitektur hibrida yang mengintegrasikan pengolahan pada domain spasial, frekuensi, dan skala secara simultan. Realisasi teknis sistem ini diwujudkan melalui pengembangan purwarupa perangkat lunak berbasis Python yang ditunjukkan pada Gambar 2. Antarmuka tersebut menyediakan kontrol terpadu bagi pengguna untuk penyisipan *watermark* serta melakukan simulasi serangan digital dalam satu alur kerja yang sistematis.



Gambar 2. Tampilan antarmuka sistem saat memproses dataset video

Arsitektur sistem ini menggunakan pendekatan alur kerja tunggal yang menggabungkan kemampuan manipulasi matriks untuk pemrosesan citra dan efisiensi *muxing* multimedia untuk sinkronisasi audio-video. Alur kerja sistem secara menyeluruh diilustrasikan pada Gambar 3, yang menunjukkan urutan proses dari dekomposisi multimedia hingga rekonstruksi final.



Gambar 3. Arsitektur Terintegrasi Sistem Watermarking Hibrida

Proses implementasi dilakukan melalui lima tahapan teknis terintegrasi:

1) Dekomposisi Multimedia dan Transformasi Ruang Warna

Proses diawali dengan pemisahan aliran audio dan visual menggunakan bantuan pustaka pemrosesan multimedia berbasis *Open Source Computer Vision Library* (OpenCV), yang menyediakan dukungan efisien untuk pengolahan citra

dan video dalam lingkungan pemrograman Python [22]. Aliran visual yang terdiri dari rangkaian *frame* dalam format BGR kemudian dikonversi ke ruang warna YCrCb. Pemilihan ruang warna ini didasarkan pada prinsip pemrosesan citra berbasis komponen warna, di mana citra direpresentasikan dalam beberapa kanal yang dapat dimanipulasi secara terpisah [23]. Fokus utama penyisipan dilakukan pada saluran luminans (Y), yang secara matematis ditransformasikan dari ruang warna RGB melalui persamaan:

$$Y = 0{,}299R + 0{,}587G + 0{,}114B$$

Pemisahan ini memungkinkan sistem memanipulasi intensitas cahaya tanpa merusak kroma asli video secara drastis, sehingga menjaga fidelitas visual.

2) Penyatuan Piksel pada Jalur Spasial

Setelah saluran Y dipisahkan, sistem melakukan penyisipan watermark melalui teknik *Alpha Blending*. Jalur ini menangani aspek visibilitas logo secara langsung pada koordinat piksel (x,y). Skema penggabungan diatur melalui persamaan :

$$I_{out}(x,y) = (1 - \alpha) \cdot I_{src}(x,y) + \alpha \cdot I_{wm}(x,y)$$

Dalam hal ini, I_{out} merupakan intensitas piksel hasil, I_{src} adalah piksel *frame* asli, I_{wm} adalah piksel logo, dan α adalah koefisien transparansi. Sistem nereapkan strategi diferensiasi nilai α: pada saluran luminans digunakan $\alpha = 0{,}55$ untuk menjamin tingkat keterbacaan, sedangkan pada saluran krominans digunakan $\alpha = 0{,}85$ guna mempertahankan integritas warna asli logo. Sebagaimana diperlihatkan pada Gambar 4, penyisipan tanda air terbukti tidak merusak informasi visual orisinil. Detail tekstur video asli tetap terlihat jelas menembus lapisan logo, membuktikan bahwa algoritma pencampuran piksel bekerja efektif mempertahankan estetika konten.

Gambar 4. Komparasi Visual Frame : (kanan) Frame Asli Bersih, (kiri) Frame dengan Watermark. Terlihat transparansi logo memungkinkan detail visual video di belakangnya tetap terjaga tanpa penutupan total.

3) Penguatan Jalur Frekuensi (*Block-based* DCT)

Jalur hibrida kedua bekerja dengan membagi saluran Y menjadi blok-blok berukuran 8×8 piksel dan mengubahnya ke domain frekuensi menggunakan *2D-Discrete Cosine Transform* (2D-DCT). Untuk menjamin presisi komputasi ortogonal, sistem memanfaatkan fungsi 'cv2.dct()' yang mengimplementasikan rumus transformasi :

$$F(u,v) = \frac{1}{4}C(u)C(v)\sum_{x=0}^{7}\sum_{x=0}^{7} f(x,y)cos\left[\frac{(2x+1)u\pi}{16}\right]cos\left[\frac{(2y+1)v\pi}{16}\right]$$

Sistem kemudian melakukan modifikasi pada koefisien frekuensi rendah $(u, v \in \{0,1\})$ untuk menyisipkan energi *watermark* yang tangguh terhadap kuantisasi kompresi. Setelah tahap penguatan selesai, data dikembalikan ke domain spasial melalui fungsi *Inverse DCT* atau 'cv2.idct()'. Tahapan ini menjamin bahwa identitas hak cipta tetap bertahan di dalam struktur frekuensi fundamental video meskipun terjadi penurunan *bitrate* yang signifikan.

4) Redundansi Multiskala

Ketahanan terhadap serangan pengubahan ukuran atau *resizing* dan gangguan sinyal ditingkatkan melalui teknik *Gaussian Pyramid*. Proses ini dilakukan secara sistematis melalui fungsi 'cv2.pyrDown()' untuk operasi *downsampling* dan 'cv2.pyrUp()' untuk rekonstruksi skala. Strategi dekomposisi ini memungkinkan sistem menyisipkan informasi *watermark* secara redundan pada berbagai tingkat resolusi piramida citra. Dengan mendistribusikan data pada level resolusi yang berbeda, logo tetap dapat terdeteksi secara matematis melalui metrik pHash meskipun video mengalami interpolasi piksel akibat proses *downscaling* atau gangguan derau acak.

5) Integrasi Kanal dan Penyatuan Multimedia

Setelah proses hibrida pada saluran Luminans (Y) selesai, sistem mengintegrasikan kembali saluran tersebut dengan saluran krominans asli (Cr dan Cb). Tahap akhir melibatkan proses *remuxing* menggunakan FFmpeg untuk menyatukan kembali rangkaian *frame* visual yang telah diproses dengan aliran audio asli. Tahapan ini menjamin sinkronisasi audio-video tetap presisi dan menghasilkan produk final yang tersimpan secara terorganisir dalam direktori keluaran sistem.

B. Prosedur Evaluasi dan Validasi Internal

Guna menjamin validitas data dan memenuhi standar *reproducibility* dalam riset informatika, sistem evaluasi menerapkan protokol *Internal Validation* yang ketat. Prosedur ini diawali dengan penetapan definisi operasional metrik yang menjadi tolok ukur keberhasilan sistem. Rincian metrik, deskripsi teknis, serta tujuan pengukurannya dirangkum dalam Tabel 2.

Tabel 2. Definisi Operasional Metrik Evaluasi

Metrik	Deskripsi Teknis	Tujuan Pengukuran	Skor Ideal
pHash	Perceptual hash 32 x 32 bit menggunakan Hamming Distance	Mendeteksi kemiripan fitur visual secara global	0,0 - 1,0. Mendekati 1,0 dianggap sangat bagus
SSIM	Pengukuran struktur berbasis patch 96 x 96 dengan stride 48	Menilai degradasi kualitas gambar (luminans, kontras, struktur)	0,0 - 1,0. Nilai > 0,90 dianggap sangat baik
Histogram	Korelasi distribusi warna pada ruang warna HSV yang dinormalisasi	Mendeteksi distorsi akibat filter atau kompresi	0,0 - 1,0. Nilai > 0,90 menunjukkan konsistensi warna yang sangat tinggi
MSE Global	Rata - rata selisih kuadrat piksel pada seluruh area bingkai	Menghitung deviasi matematis mutlak/kerusakan data total	0 - ∞.Semakin mendekati 0 semakin baik.
WM Area MSE	MSE spesifik pada ROI pojok kanan atas	Mendeteksi tingkat kerusakan atau hilangnya logo watermark	0 - ∞.Semakin mendekati 0 semakin baik.

Implementasi dari metrik-metrik tersebut dijalankan melalui skrip evaluasi otomatis yang menerapkan lima mekanisme validasi utama:

1. *Fixed Frame Indexing*

   Evaluasi dilakukan secara konsisten pada indeks frame ke-10 (indeks 9). Mekanisme ini krusial untuk menghindari *timestamp drift* atau pergeseran frame akibat variasi frame rate (VFR) atau kehilangan *frame* proses kompresi dan konversi. Hal ini memastikan bahwa perbandingan antara master dan *attacked video* dilakukan pada posisi temporal yang identik.

2. *Patch-based* SSIM

   Berbeda dengan SSIM standar yang menghitung rata-rata global, penelitian ini menggunakan pendekatan berbasis patch 96×96 piksel dengan stride 48. Teknik ini bekerja seperti "kaca pembesar" yang memeriksa bagian-bagian kecil citra secara tumpang tindih. Pendekatan ini jauh lebih sensitif dalam mendeteksi degradasi lokal pada area logo, sehingga mampu menangkap kerusakan struktur kecil akibat interpolasi yang sering kali tidak terdeteksi oleh SSIM global.

3. *Targeted ROI Extraction* (WM *Area* MSE)

   Validasi difokuskan secara spesifik pada *Region of Interest* (ROI) melalui algoritma ekstraksi koordinat yang telah dikembangkan. Sistem mengekstraksi koordinat piksel yang sama persis dengan logika penempatan watermark asli yaitu kanan atas dengan safe margin 5%. Pemisahan antara MSE secara global dan WM Area MSE memungkinkan peneliti untuk membedakan antara penurunan kualitas video secara umum dengan kerusakan spesifik pada identitas hak cipta.

4. *Multidimensional Metric Cross-Check*

   Sistem menggunakan kombinasi empat metrik yang berbeda karakter yaitu pHash untuk kemiripan fitur frekuensi, SSIM untuk integritas struktur, Histogram untuk distribusi warna, dan MSE untuk selisih matematis piksel. Penggunaan metrik multidimensi ini berfungsi sebagai validasi silang, misalnya, jika SSIM rendah namun pHash tetap tinggi, ini mengonfirmasi adanya perubahan struktur seperti pada kasus *resizing* tanpa merusak identitas visual secara keseluruhan.

5. *Automated Pipeline & Statistical Consistency*

   Proses evaluasi dijalankan secara otomatis melalui pemindaian rekursif terhadap 10 sampel video di seluruh folder serangan. Mekanisme ini menghilangkan bias manusia dalam pengambilan sampel data. Data yang terkumpul dikompilasi langsung ke dalam format CSV dan XLSX, memastikan integritas data dari tahap ekstraksi hingga tahap analisis statistik.

C. Skenario Simulasi Serangan

Bagian ini memberikan konteks operasional terhadap data numerik yang dihasilkan. Simulasi serangan tidak hanya dipandang sebagai gangguan teknis, tetapi sebagai skenario uji untuk memvalidasi performa algoritma hibrida dalam berbagai kondisi distribusi konten. Skenario ini dikelompokkan menjadi tiga fokus pengujian utama untuk memudahkan interpretasi hasil.

1. Skenario Gangguan Sinyal dan Transmisi

Skenario ini mensimulasikan kondisi di mana video mengalami degradasi kualitas akibat keterbatasan *bandwidth* atau interferensi saluran. Penggunaan *Gaussian Noise* dan kompresi H.264 yaitu CRF 32 dan 40 bertujuan untuk menguji apakah penguatan pada domain frekuensi (DCT) mampu mempertahankan integritas *watermark* saat detail piksel mengalami "penyederhanaan" matematis. Keberhasilan dalam skenario ini dapat diukur melalui stabilitas nilai pHash yang merepresentasikan identitas visual global.

2. Skenario Transformasi Geometri dan Skala

Skenario ini dirancang untuk menguji ketahanan sistem terhadap perubahan dimensi dan komposisi *frame*. Pada skenario *resizing*, fokus pengujian adalah efektivitas

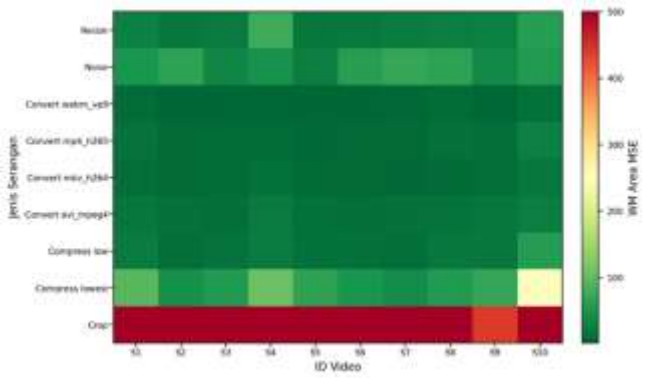
Gaussian Pyramid dalam menjaga redundansi logo pada berbagai skala. Sementara itu, skenario *cropping* sebesar 12,5% pada setiap sisi merupakan skenario "kegagalan paksa" untuk mengidentifikasi batas toleransi koordinat spasial statis terhadap hilangnya referensi *Safe Area* sesuai standar EBU R 95.

3. Skenario Interoperabilitas Kontainer

Skenario terakhir melibatkan perubahan format kontainer dan *codec* seperti AVI, MKV, WebM dan H.265. Skenario ini sangat krusial untuk memastikan bahwa tanda air yang disisipkan bersifat *agnostic* atau tidak bergantung pada jenis kompresor tertentu. Pengujian pada *codec* H.265 (HEVC) khususnya, bertujuan untuk melihat bagaimana skema hibrida menghadapi algoritma kompresi modern yang memiliki tingkat efisiensi dan kompleksitas kuantisasi yang jauh lebih tinggi dibanding standar sebelumnya.

D. Analisis Hasil Kuantitatif dan Statistik

Pengujian Eksperimen dilakukan terhadap sepuluh sampel video dengan karakteristik visual yang bervariasi untuk menguji reliabilitas algoritma hibrida. Seluruh data diekstraksi secara otomatis untuk meminimalkan bias manusia. Distribusi *error* divisualisasikan dalam bentuk peta panas atau *heatmap* pada Gambar 5. Visualisasi ini menerapkan ambang batas visual pada nilai WM Area MSE > 500 untuk membedakan secara tegas antara degradasi minor dan kegagalan deteksi.



Gambar 5. Heatmap Distribusi Error WM Area MSE. Warna merah pekat pada baris 'Cropped' menunjukkan kegagalan deteksi masif, kontras dengan baris 'Converted' yang dominan hijau (aman).

Rekapitulasi performa sistem yang menyajikan nilai rata-rata dari seluruh pengujian dirangkum dalam Tabel 3.

Tabel 3. Ringkasan Hasil Pengujian Ketahanan

Kategori Serangan	Rata - rata pHash	Rata - rata SSIM	Rata - rata Histogram	Rata - rata MSE	Rata - rata WM MSE	Status Ketahanan
Resized	0,993	0,566	0,997	13,556	32,501	Tangguh
Noise	0,981	0,662	0,780	43,524	51,120	Tangguh
Convert webm	0,994	0,988	0,995	3,637	4,693	Sangat Tangguh
Convert h265	0,993	0,982	0,990	7,441	10,291	Sangat Tangguh
Convert mkv	0,995	0,989	0,999	4,795	9,073	Sangat Tangguh
Convert avi	0,994	0,983	0,949	5,771	15,383	Sangat Tangguh
Compress low	0,992	0,975	0,995	12,422	20,591	Sangat Tangguh
Compress lowest	0,980	0,918	0,937	57,963	83,965	Tangguh
Crop	0,838	0,588	0,930	2424,889	2304,230	Gagal

Data pada Tabel 3 menunjukkan tingkat konsistensi yang sangat tinggi pada kategori serangan administratif yaitu konversi dan kompresi. Namun, terdapat fluktuasi signifikan pada metrik WM *Area* MSE untuk serangan *cropping*, di mana Standar Deviasi (σ) yang dihasilkan mencapai angka yang sangat lebar. Hal ini mengindikasikan bahwa dampak serangan geometri makro sangat bergantung pada komposisi piksel dan resolusi awal video yang digunakan.

1. Analisis pHash terhadap Ketahanan Perseptual

Metrik Perceptual Hash (pHash) menunjukkan stabilitas yang impresif dengan nilai di atas 0,98 untuk hampir seluruh skenario serangan, kecuali *cropping*. Fenomena ini terjadi karena mekanisme pHash mereduksi bingkai video menjadi *grid* frekuensi rendah berukuran 32×32. Karena serangan kompresi dan konversi format seperti H.265 dan WebM)secara dominan hanya memanipulasi atau membuang detail frekuensi tinggi , "sidik jari" visual video tetap dianggap identik oleh sistem pendeteksi. Hal ini membuktikan bahwa metode hibrida DCT-Spasial berhasil mempertahankan esensi visual konten di bawah tekanan *transcoding*.

2. Interpretasi Teknis Lonjakan MSE pada Serangan *Resizing*

Ditemukan anomali di mana serangan *resizing* menghasilkan WM Area MSE yang lebih tinggi yaitu 32,501 dibandingkan serangan konversi misal WebM dengan nilai MSE 4,693. Secara teknis, hal ini dipicu oleh efek interpolasi *bicubic*. Saat video diubah ukurannya misal dari Full HD ke HD, piksel pada area watermark dihitung ulang berdasarkan bobot piksel tetangganya. Ketika proses evaluasi melakukan *resizing* balik untuk menyamakan dimensi bingkai, terjadi akumulasi kesalahan pembulatan koordinat piksel. Kendati indikator SSIM mencatat nilai 0,566 yang merepresentasikan kualitas visual yang cukup baik, rumus MSE memberikan penalti matematis yang signifikan terhadap setiap pergeseran intensitas piksel.

3. Analisis Kerentanan *Cropping* dan Paradoks Ketahanan

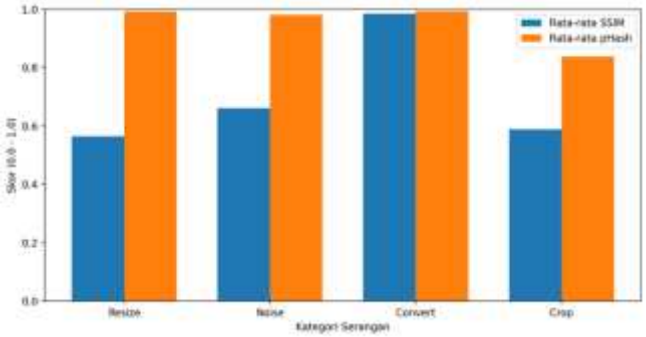
Temuan paling krusial dalam penelitian ini adalah munculnya paradoks ketahanan atau *robustness paradox*. Merujuk pada data Tabel 3, video hasil *cropping* terbukti

tetap mempertahankan fidelitas warna yang sangat baik dengan nilai Histogram mencapai 0,930 serta struktur visual yang masih layak dengan skor SSIM sebesar 0,588. Namun, dari perspektif keamanan terjadi kegagalan total yang diindikasikan oleh lonjakan nilai WM Area MSE hingga mencapai angka 2304,23. Ilustrasi teknis mengenai penyebab kegagalan ini dapat dilihat pada Gambar 6, di mana area pemotongan menghilangkan referensi spasial logo.

Gambar 6. Desinkronisasi Spasial: Area Watermark (Hijau) tereliminasi sepenuhnya oleh pemotongan margin 12,5% (Merah), menyebabkan kegagalan deteksi.

Secara teknis, paradoks ini dipicu oleh desinkronisasi spasial. Mengingat sistem menempatkan *watermark* pada margin 5%, serangan pemotongan sebesar 12,5% pada setiap sisi secara otomatis mengeliminasi seluruh koordinat piksel *watermark* sebagaimana diilustrasikan pada Gambar 6. Dengan kondisi tersebut, penyerang berhasil memisahkan identitas hukum dari nilai ekonomi video tanpa menurunkan kualitas visual konten secara signifikan. Temuan ini selaras dengan pernyataan Cox et al. bahwa transformasi geometris seperti *cropping* menyebabkan desinkronisasi *watermark* dan menjadi tantangan utama bagi sistem penandaan air statis yang tidak dilengkapi mekanisme registrasi atau sinkronisasi ulang posisi [24].

Sebagai penutup analisis, ringkasan komparatif antara kualitas visual melalui metrik SSIM dan ketahanan identitas menggunakan *pHash* untuk setiap kategori serangan disajikan pada Gambar 7. Grafik ini mempertegas divergensi performa yang ekstrem pada kategori *Cropping*.



Gambar 7. Perbandingan Rata-rata Skor Kualitas (SSIM) dan Identitas (pHash). Terlihat ketimpangan signifikan pada kategori Cropping dibanding kategori lainnya.

E. Rekomendasi dan Arah Pengembangan Riset

Berdasarkan hasil evaluasi, arsitektur hibrida yang menyinergikan *Alpha Blending* pada domain spasial dan DCT pada domain frekuensi, serta diperkuat dengan teknik multiskala *Gaussian Pyramid*, terbukti sangat efisien dan tangguh terhadap variasi dimensi maupun kompresi. Namun, guna menjawab tantangan spesifik pada serangan geometri ekstrem seperti *cropping*, penelitian selanjutnya disarankan untuk menerapkan *Dynamic Watermark* sebagai solusi taktis. Mekanisme pergeseran koordinat logo secara temporal ini akan mempersulit upaya penghilangan *watermark* melalui pemotongan area statis tanpa merusak estetika visual subjek utama video.

Selanjutnya, eksplorasi komparatif yang lebih mendalam pada domain frekuensi dapat dilakukan menggunakan metode *Discrete Wavelet Transform* (DWT) atau *Singular Value Decomposition* (SVD). Meskipun pendekatan ini menuntut sumber daya komputasi yang lebih tinggi dibandingkan efisiensi metode DCT yang digunakan saat ini, teknik *spread spectrum* yang dimilikinya menawarkan penyebaran data yang lebih luas ke seluruh *sub-band* frekuensi. Hal ini secara teoritis berpotensi menutup celah kerentanan desinkronisasi geometris, menjadikannya alternatif yang layak untuk skenario perlindungan yang memprioritaskan ketahanan struktur di atas kecepatan pemrosesan.

IV. KESIMPULAN

Berdasarkan Penelitian ini menyimpulkan bahwa implementasi sistem *Hybrid Visible Watermarking* berbasis Python berhasil membuktikan efektivitas arsitektur yang menyinergikan pengolahan domain spasial, transformasi frekuensi (DCT), serta pendekatan multiskala (*Gaussian Pyramid*) dalam menjaga keseimbangan optimal antara fidelitas visual dan ketahanan data. Berdasarkan evaluasi kuantitatif, sistem menunjukkan performa tangguh dengan mempertahankan nilai SSIM di atas 0,91 dan pHash di atas 0,97 saat menghadapi serangan administratif seperti kompresi H.264 dan konversi format. Secara spesifik, penerapan teknik multiresolusi tersebut memberikan kontribusi vital dalam menjaga stabilitas identitas *watermark* terhadap manipulasi dimensi, di mana redundansi data pada berbagai level resolusi terbukti mampu menoleransi efek interpolasi piksel tanpa merusak keterbacaan logo secara matematis.

Meskipun sistem menunjukkan ketahanan superior terhadap gangguan sinyal, penelitian ini mengidentifikasi batasan fundamental berupa fenomena "Paradoks Ketahanan" pada serangan geometri ekstrem. Temuan menunjukkan bahwa *cropping* sebesar 12,5% pada setiap sisi mengakibatkan kegagalan deteksi total yang ditandai dengan lonjakan nilai WM Area MSE hingga 2.304,23, kendati kualitas visual video secara umum masih terjaga dengan baik. Kegagalan ini mengonfirmasi bahwa desinkronisasi spasial akibat hilangnya referensi koordinat

tetap menjadi kelemahan inheren pada metode *visible watermarking* statis yang memisahkan aspek perlindungan hak cipta dari nilai ekonomi konten. Guna mengatasi kerentanan ini, penelitian selanjutnya direkomendasikan untuk menerapkan mekanisme *Dynamic Watermark* atau mengeksplorasi metode domain frekuensi tingkat lanjut seperti *Discrete Wavelet Transform - Singular Value Decomposition* (DWT-SVD) untuk menyebarkan informasi kepemilikan ke seluruh spektrum bingkai citra agar lebih persisten terhadap pemotongan area.

DAFTAR PUSTAKA

[1] Sindy Ariyaningsih, A. Ari Andrianto, Adri Surya Kusuma, Rina Arum Prastyanti "Korelasi Kejahatan Siber dengan Percepatan Digitalisasi di Indonesia," *Justisia J. Ilmu Huk. Univ. Pas.*, vol. 1, no. 1, pp. 8–10, 2023, doi: https://doi.org/10.56457/jjih.v1i1.38.

[2] R. Harits Anandito, R. Januar, T. Aswin Aswangga, H. Abednego Lubis, and Mustaqim, "Analisa Tentang Pembajakan Video Dalam Perspektif Hak Atas Kekayaan Intelektual," *J. Media Akad.*, vol. 2, no. 1, pp. 406–422, 2024.

[3] Didi Rosiyadi, *Teknologi Watermarking Untuk Mendukung Keamanan Siber Di Indonesia*. 2024. doi: 10.55981/brin.1260.

[4] S. Supiyandi *et al.*, "Application of invisible image watermarking," *Int. J. Eng. Technol.*, vol. 7, no. 3.2 Special Issue 2, pp. 760–762, 2018, doi: 10.14419/ijet.v7i3.2.18749.

[5] Mukhammad Solikhin, Y. Pratama, Purnama Pasaribu, Josua Rumahorbo, and Bona Simanullang, "Analisis Watermarking Menggunakan Metode Discrete Cosine Transform (DCT) dan Discrete Fourier Transform (DFT)," *J. Sist. Cerdas*, vol. 5, no. 3, pp. 155–170, 2022, doi: 10.37396/jsc.v5i3.192.

[6] I. Fi and E. Ujianto, "Invisible Watermarking Citra Digital Menggunakan Kombinasi Metode Discrete Cosine Transform Dan Discrete Wavelet Transform," *J. Nas. Pendidik. Tek. Inform. (JANAPATI)*, vol. 8, no. 3, pp. 261–271, 2019.

[7] S. D. A. Anna Baita, Rohmatullah Batik Firmansyah, "Optimasi Nilai Imperceptibility Pada Watermarking Citra Warna Berbasis DCT-DWT," *JIPI (Jurnal Ilm. Penelit. dan Pembelajaran Inform.*, vol. 10, p. 622, 2025.

[8] W. Chen, N. Ren, C. Zhu, Q. Zhou, T. Seppänen, and A. Keskinarkaus, "Screen-cam robust image watermarking with feature-based synchronization," *Appl. Sci.*, vol. 10, no. 21, pp. 1–27, 2020, doi: 10.3390/app10217494.

[9] H. Jurnal, M. Saifudin, H. W. Progdi, and K. Akuntansi, "Jurnal Teknik Informatika Dan Teknologi Informasi Rancang Bangun Sistem Digitalisasi Dokumen Menggunakan Metode Visible Watermark Di Kantor Urusan Agama (Kua) Kecamatan Sayung," *J. Jutiti*, vol. 1, no. 3, pp. 1–7, 2021.

[10] F. Masykur, "Implementasi Watermarking Metode LSB Pada Citra Guna Perlindungan Karya Cipta," *ijns.org Indones. J. Netw. Secur.*, vol. 5, no. 3, pp. 2302–5700, 2016.

[11] A. Gimnastiar, L. S. Harahap, and R. Abdillah, "Implementasi Watermarking Pada Gambar Menggunakan Matlab Untuk Mencegah Plagiarisme Laporan Praktikum," *J. Teknol. Dan Sist. Inf. Bisnis*, vol. 7, no. 3, pp. 372–377, 2025, doi: 10.47233/jteksis.v7i3.1970.

[12] M. Waruwu, S. N. Pu`at, P. R. Utami, E. Yanti, and M. Rusydiana, "Metode Penelitian Kuantitatif: Konsep, Jenis, Tahapan dan Kelebihan," *J. Ilm. Profesi Pendidik.*, vol. 10, no. 1, pp. 917–932, 2025, doi: 10.29303/jipp.v10i1.3057.

[13] S. Simanjuntak, "Implementasi Metode Taboo Code Untuk Kompresi File Video," *Explorer (Hayward).*, vol. 2, no. 1, pp. 32–38, 2022, doi: 10.47065/explorer.v2i1.156.

[14] T. H. Soe and M. Slavkovik, "A content-aware tool for converting videos to narrower aspect ratios," *IMX 2022 - Proc. 2022 ACM Int. Conf. Interact. Media Exp.*, pp. 109–119, 2022, doi: 10.1145/3505284.3529970.

[15] K. Umam and B. S. Negara, "Deteksi Obyek Manusia Pada Basis Data Video Menggunakan Metode Background Subtraction Dan Operasi Morfologi," *J. CoreIT J. Has. Penelit. Ilmu Komput. dan Teknol. Inf.*, vol. 2, no. 2, p. 31, 2016, doi: 10.24014/coreit.v2i2.2391.

[16] A. Yulius, Lina, and C. Adipianto, "Pemanfaatan Library FFMPEG Untuk Perancangan Aplikasi Konversi File Video Ke Format GIF Berbasis Android," *J. InTekSis*, vol. 7, no. 2, pp. 72–82, 2020.

[17] J. Ulfah and N. Nurdin, "Implementasi Metode Deteksi Tepi Canny Untuk Menghitung Jumlah Uang Koin Dalam Gambar Menggunakan Opencv," *J. Inform. dan Tek. Elektro Terap.*, vol. 11, no. 3, pp. 420–426, 2023, doi: 10.23960/jitet.v11i3.3147.

[18] R. M. Rachman, A. Sobandi, and A. Wahyudin, "Penggunaan Aplikasi Pendeteksi Plagiarisme Image Sebagai Fasilitas Pendukung Otomatisasi Perkantoran," *J. MANAJERIAL*, vol. 21, no. 1, pp. 35–48, 2022, doi: 10.17509/manajerial.v21i1.42652.

[19] H. B. Sumarna, E. Utami, and A. D. Hartanto, "Tinjauan Literatur Sistematik tentang Structural Similarity Index Measure untuk Deteksi Anomali Gambar," *Creat. Inf. Technol. J.*, vol. 7, no. 2, p. 75, 2021, doi: 10.24076/citec.2020v7i2.248.

[20] K. Aviantoro and Y. Darnita, "Implementasi Wiener, Contrast Stretching, Sharpening Filter Pada Citra Semangka Menggunakan Mse,Rmse, Dan

Psnr," *Djtechno J. Teknol. Inf.*, vol. 5, no. 2, pp. 195–205, 2024, doi: 10.46576/djtechno.v5i2.4613.

[21] M. M.Elsheh and S. A.Eltomi, "Content Based Image Retrieval using Color Histogram and Discrete Cosine Transform," *Int. J. Comput. Trends Technol.*, vol. 67, no. 9, pp. 25–31, 2019, doi: 10.14445/22312803/ijctt-v67i9p105.

[22] L. Riani *et al.*, "SiCitra: Aplikasi Berbasis Web untuk Pemrosesan Citra Digital Menggunakan OpenCV," *J. Inform. Upgris*, vol. 10, no. 2, pp. 39–46, 2024, doi: 10.26877/jiu.v10i2.20924.

[23] B. C. Wibowo, F. Nugraha, and A. P. Utomo, "Uji Deteksi Objek Bentuk Bola Dengan Menerapkan Metode Circular Hough Transform," *J. Inform. Upgris*, vol. 7, no. 1, 2021, doi: 10.26877/jiu.v7i1.8309.

[24] I. J. Cox, J. Kilian, F. T. Leighton, and T. Shamoon, "Secure spread spectrum watermarking for multimedia," *IEEE Trans. Image Process.*, vol. 6, no. 12, pp. 1673–1687, 1997, doi: 10.1109/83.650120.

LAMPIRAN

Tabel A Rekapitulasi Hasil Pengujian 10 Sampel Video

Video ID	Jenis Serangan	pHash score	SSIM score	Histogram score	MSE	WM Area MSE
sample1	resized	0,988	0,483	0,996	18,535	29,582
	noise	0,973	0,713	0,863	51,051	50,474
	converted Webm	0,988	0,983	0,996	5,621	7,987
	converted H265	0,993	0,975	0,993	9,618	14,784
	converted MKV	0,993	0,981	0,998	7,435	9,603
	converted AVI	0,99	0,974	0,977	10,353	16,99
	compressed Low	0,993	0,964	0,996	15,276	24,431
	compressed Lowest	0,973	0,871	0,975	69,092	93,769
	cropped	0,796	0,477	0,911	3030,265	2632,005
sample2	resized	0,99	0,522	0,999	7,47	19,167
	noise	0,969	0,615	0,609	35,615	66,131
	converted Webm	0,993	0,986	0,999	2,735	2,816
	converted H265	0,988	0,978	0,997	5,153	5,65
	converted MKV	0,99	0,989	1	3,144	5,873
	converted AVI	0,988	0,978	0,975	3,979	11,348
	compressed Low	0,987	0,972	0,999	8,304	11,059
	compressed Lowest	0,968	0,925	0,986	27,675	45,132
	cropped	0,832	0,438	0,851	1029,311	1484,771
sample3	resized	0,99	0,661	0,998	5,388	21,954
	noise	0,978	0,819	0,951	29,081	33,161
	converted Webm	0,993	0,99	0,997	2,32	2,829
	converted H265	0,991	0,985	0,994	4,363	7,228
	converted MKV	0,992	0,987	0,998	4,046	7,582
	converted AVI	0,99	0,985	0,968	3,922	10,954
	compressed Low	0,99	0,979	0,995	6,801	13,399
	compressed Lowest	0,973	0,936	0,907	31,268	57,016
	cropped	0,792	0,687	0,893	1454,948	1419,277
sample4	resized	0,999	0,454	1	4,707	76,318
	noise	0,998	0,576	0,571	30,016	46,587
	converted Webm	0,999	0,993	1	1,404	3,175
	converted H265	0,999	0,99	1	2,254	8,718
	converted MKV	0,999	0,994	1	1,481	12,799
	converted AVI	0,999	0,989	1	2,584	22,325
	compressed Low	0,999	0,99	1	2,909	24,621
	compressed Lowest	0,999	0,971	0,998	12,252	107,576
	cropped	0,946	0,549	0,998	1944,707	1621,407
sample5	resized	0,998	0,741	1	10,207	19,907
	noise	0,998	0,442	0,557	14,367	24,963
	converted Webm	0,999	0,999	1	0,407	1,346
	converted H265	0,999	0,998	1	0,768	3,781
	converted MKV	0,999	0,999	1	0,686	6,308
	converted AVI	1	0,998	1	0,883	11,474
	compressed Low	0,998	0,997	1	1,952	12,818
	compressed Lowest	0,994	0,989	1	10,547	66,266
	cropped	0,918	0,717	1	4202,283	1323,845
sample6	resized	0,991	0,834	0,995	9,669	20,768
	noise	0,958	0,572	0,83	63,883	60,975
	converted Webm	0,988	0,989	0,981	3,024	2,32
	converted H265	0,988	0,986	0,96	5,347	6,076
	converted MKV	0,996	0,992	0,998	3,146	5,745
	converted AVI	0,988	0,986	0,953	4,839	10,512
	compressed Low	0,989	0,985	0,98	7,077	12,049
	compressed Lowest	0,966	0,962	0,81	35,324	50,562
	cropped	0,812	0,857	0,888	1024,763	1282,153
sample7	resized	0,992	0,761	0,992	16,702	24,031
	noise	0,964	0,584	0,886	68,747	70,812
	converted Webm	0,989	0,986	0,989	5,14	3,51
	converted H265	0,985	0,974	0,968	13,325	6,72
	converted MKV	0,993	0,989	0,998	5,475	4,907
	converted AVI	0,992	0,984	0,917	5,807	12,016
	compressed Low	0,99	0,964	0,992	20,957	10,112
	compressed Lowest	0,981	0,895	0,89	86,63	40,477
	cropped	0,833	0,814	0,893	2195,26	1012,05
sample8	resized	0,997	0,532	0,993	11,724	26
	noise	0,994	0,69	0,768	56,224	64,357
	converted Webm	0,997	0,979	0,993	5,466	8,155
	converted H265	0,998	0,976	0,996	7,04	11,892
	converted MKV	0,995	0,983	0,999	5,124	6,73
	converted AVI	0,997	0,973	0,947	7,714	14,224
	compressed Low	0,996	0,964	0,997	12,333	19,287
	compressed Lowest	0,99	0,902	0,957	48,172	57,576
	cropped	0,943	0,6	0,959	1562,437	4397,782
sample9	resized	0,996	0,467	0,998	11,786	27,425
	noise	0,992	0,831	0,921	27,983	37,287
	converted Webm	1	0,992	0,998	1,888	2,533
	converted H265	0,999	0,987	0,992	4,7	10,072
	converted MKV	1	0,99	0,999	3,604	10,788
	converted AVI	0,998	0,985	0,902	4,647	17,519
	compressed Low	0,997	0,983	0,997	7,515	19,813
	compressed Lowest	0,991	0,943	0,928	41,254	70,484
	cropped	0,733	0,509	0,921	4355,873	440,992
sample10	resized	0,985	0,201	0,997	39,374	59,858
	noise	0,99	0,774	0,839	58,272	56,451
	converted Webm	0,995	0,984	0,999	8,363	12,262
	converted H265	0,99	0,971	0,997	21,842	27,988
	converted MKV	0,989	0,981	0,999	13,809	20,398
	converted AVI	0,993	0,976	0,846	12,981	26,468
	compressed Low	0,983	0,952	0,997	41,091	58,317
	compressed Lowest	0,963	0,783	0,916	217,417	250,787
	cropped	0,771	0,236	0,981	3449,046	7428,019