

# Penggunaan Algoritme *Singular Value Decomposition* pada *Video Watermarking*

Gloryanson Ginting  
Sekolah Teknik Elektro dan Informatika  
Institut Teknologi Bandung  
Bandung, Indonesia  
email@gmail.com

Rinaldi Munir  
Sekolah Teknik Elektro dan Informatika  
Institut Teknologi Bandung  
Bandung, Indonesia  
rinaldi@informatika.org

**Abstrak**— *Media sosial adalah teknologi komunikasi yang menjadi salah satu aspek kehidupan manusia pada abad ke-21. Media sosial umumnya digunakan oleh pengguna untuk menyebarkan konten baik dalam bentuk gambar maupun video. Masalah yang muncul akibat media sosial adalah pelanggaran hak cipta dengan menyebarkan gambar maupun video tanpa seizin pemilik hak cipta. Salah satu solusi untuk masalah tersebut adalah penggunaan watermark untuk mempermudah proses identifikasi video yang memiliki hak cipta di media sosial. Penggunaan teknik steganografi untuk menanamkan watermark pada gambar maupun video disebut dengan watermarking. Singular Value Decomposition (SVD) adalah salah satu algoritme watermarking yang memiliki keunggulan berupa: kasat mata, tahan terhadap serangan, serta memiliki waktu komputasi yang cepat. Hasil eksperimen pada penelitian ini menemukan bahwa proses ekstraksi watermark algoritme SVD memiliki kualitas yang relatif rendah dengan nilai rata-rata PSNR 16,5 db. Hal ini dikarenakan kualitas watermark memiliki korelasi dengan bitrate video yang digunakan. Penelitian ini juga mendapatkan bahwa algoritme SVD memiliki ketahanan terhadap serangan noise, filter, trim, dan compression. Selain itu, hasil eksperimen menemukan bahwa algoritme SVD memiliki kinerja yang relatif baik dengan waktu komputasi yang cepat dengan rata-rata waktu 7 menit 54 detik. Kinerja algoritma ekstraksi watermark relatif cepat dengan waktu rata-rata yaitu 7,597 detik untuk ekstraksi video tanpa serangan, 7,387 detik untuk ekstraksi video telah mengalami serangan filter, 7,485 detik untuk ekstraksi video telah mengalami serangan noise, dan 7,532 detik untuk ekstraksi video telah mengalami serangan compression.*

**Kata kunci**—*media sosial, steganografi, watermarking, Singular Value Decomposition (SVD)*

## I. PENDAHULUAN

Media sosial adalah teknologi komunikasi yang menjadi salah satu aspek kehidupan manusia pada abad ke-21. Media sosial umumnya digunakan oleh pengguna untuk membaca berita, berhubungan dengan teman, keluarga, maupun komunitas, serta menyertakan pendapat [1]. Pada tahun 2022, terdapat 4,76 miliar atau 59,4 persen

populasi dunia yang menggunakan media sosial [2]. Survei oleh Nurhayati (2023) mendapatkan bahwa 191,4 juta atau sekitar 68,9 persen penduduk Indonesia menggunakan media sosial, dengan rata-rata waktu yang digunakan untuk menggunakan media sosial adalah 3 jam 20 menit.

Steganografi adalah teknik menyembunyikan informasi pada suatu gambar, dokumen, maupun video [4]. Steganografi dapat digunakan untuk *watermarking*, yaitu teknik untuk mengecek keaslian suatu gambar. *Watermarking* digital menggunakan algoritme untuk menambahkan pesan rahasia yang digunakan untuk autentikasi dan menjaga integrasi data dalam bentuk *noise* sehingga tidak dapat dilacak kasat mata [5]. Penelitian *watermarking* bertujuan untuk meminimalkan pengaruh pesan rahasia pada data asli serta memastikan bahwa watermark tahan terhadap serangan-serangan pada data seperti *filter*, *noise*, dan *compression* [6].

Penelitian [7] menciptakan algoritme yang mengubah sebagian koefisien frekuensi dengan fungsi *Discrete Cosine Transform* dua dimensi (2D-DCT) untuk menghasilkan produk *watermarking* yang memiliki efek yang minimal pada isi gambar, dapat diandalkan, dan aman. Penelitian tersebut mengukur ketahanan watermark terhadap serangan dengan membandingkan beberapa algoritme lain lalu melakukan beberapa jenis serangan yaitu *crop*, *zoom*, *rotate*, *translation*, dan penambahan *noise*. Gambar-gambar hasil serangan tersebut lalu akan diukur kemiripannya dengan gambar asli dengan menggunakan metrik *Peak Signal-to-Noise Ratio* (PSNR) dan *Structural Similarity Index Measure* (SSIM). Hasil menunjukkan bahwa algoritme 2D-DCT mendapatkan rata-rata nilai PSNR sebesar 40,95 dan nilai SSIM sebesar 0,97. Penelitian [8] menggunakan *Imperialistic Competition Algorithm* (ICA) untuk mengidentifikasi lokasi pada domain spasial gambar yang cocok untuk data watermark. Penelitian tersebut mengukur ketahanan watermark terhadap serangan dengan membandingkan beberapa algoritme lain lalu melakukan beberapa jenis serangan yaitu *sharpening*, *blur*, dan penambahan *noise*. Gambar-gambar berisi watermark tersebut lalu akan diukur kemiripannya dengan gambar asli dengan menggunakan metrik PSNR dan *Mean Absolute Error* (MAE). Hasil menunjukkan bahwa ICA mendapatkan nilai PSNR sebesar 45,62 dan nilai MAE sebesar 0,0029.

Penelitian-penelitian sebelumnya belum menelusuri penggunaan *Singular Value Decomposition* (SVD) untuk proses *watermarking* pada domain frekuensi video yang

tahan terhadap serangan. Penelitian-penelitian sebelumnya juga tidak mengukur keefektifan *watermarking* untuk mencegah pelanggaran hak cipta pada media sosial. Penelitian [9] menggunakan algoritme steganografi berdasarkan SVD yang berada pada domain spasial yang hanya dapat digunakan pada gambar tanpa warna. Penelitian [10] mampu mengolah video dengan menggunakan steganografi pada domain *wavelet* sehingga memiliki kebutuhan komputasi yang rendah namun algoritme tersebut memiliki kelemahan yaitu rentan terhadap serangan.

Melihat kekurangan-kekurangan pada penelitian sebelumnya, penelitian ini mengimplementasikan algoritme SVD untuk mencegah penyebaran video tanpa seizin pemilik hak cipta pada media sosial yang aman ketika mengalami serangan. Penelitian ini bertujuan untuk menjaga hak cipta pemilik video yang disebarluaskan melalui media sosial tanpa seizin pemilik hak cipta. Penelitian ini juga akan mengevaluasi kualitas watermark serta kinerja metode yang digunakan.

Kebutuhan untuk suatu algoritme yang mampu mencegah penyebaran video di media sosial mendorong penelitian ini untuk menelusuri teknik *watermarking* pada video. Maka dari itu, penelitian dengan judul “Penggunaan Algoritme Singular Value Decomposition pada *Video watermarking*” ini diharapkan dapat menggunakan algoritme SVD untuk menyelesaikan masalah terkait dengan *Video watermarking*.

## II. STUDI LITERATUR

### A. *Video watermarking*

*Video watermarking* adalah teknik penandaan yang digunakan pada video untuk mempermudah proses identifikasi, pengaturan penggunaan maupun penyebaran, pendeteksian perubahan konten, dan perlindungan hak cipta [5]. Proses *watermarking* dibagi menjadi dua tahap, yaitu proses penanaman watermark serta proses ekstraksi watermark. *Video watermarking* menggunakan proses yang sama dengan *watermarking* pada gambar, dimana video dipecah menjadi urutan gambar atau *frame* ketika proses penanaman serta ekstraksi watermark dilaksanakan. *Watermarking* dikategorikan menjadi dua jenis berdasarkan lokasi yang digunakan untuk menyembunyikan watermark, yaitu: domain spasial dan domain frekuensi [11].

#### 1) Discrete Wavelet Transform

Discrete Wavelet Transform (DWT) adalah fungsi yang digunakan untuk kompresi data dan pemrosesan sinyal [5]. DWT merepresentasikan gambar menjadi fungsi *wavelet* yang mampu mengekstrak frekuensi dan informasi spasial gambar. DWT menggunakan dua *filter* yaitu *low-pass* dan *high-pass* untuk membagi gambar menjadi empat *subband* yaitu LL, LH, HL, dan HH. LL adalah *downsample* dari gambar awal, LH menyimpan fitur horizontal, HL menyimpan fitur vertikal, dan HH menyimpan fitur titik berfrekuensi tinggi. DWT dapat digunakan untuk menyembunyikan watermark karena DWT dapat digunakan secara multi-resolusi, tahan

terhadap serangan, dan kasat mata. Rumus matematika untuk DWT dapat dilihat pada Persamaan (1).

$$T_{m,n} = \int_{-\infty}^{\infty} x(t)\psi_{m,n}(t) dt \quad (1)$$

dengan  $m$  adalah parameter *scale*,  $n$  adalah parameter *shift*,  $x$  adalah sinyal, dan  $\Psi$  adalah fungsi basis *wavelet*.

#### 2) Serangan pada Watermark

Serangan pada watermark adalah proses yang mencoba untuk menghilangkan atau mengubah watermark yang berada pada konten digital sehingga tidak dapat dideteksi. Teknik *watermarking* yang rentan terhadap serangan merupakan teknik yang tidak *robust*. Serangan pada watermark dapat digunakan untuk mengevaluasi keefektifan teknik *watermarking* yang digunakan. Menurut penelitian [5] serangan-serangan pada watermark yang umum adalah sebagai berikut:

1. Penambahan *noise* acak
2. *Filtering*: *average filtering*, *median filtering*, dan *Gaussian lowpass filtering*
3. Geometrik: *rescaling*, *rotation*, dan *cropping*
4. *Enhancement*: *gamma correction*, *image sharpening*, dan *histogram equalization*
5. Kompresi: JPEG dan JPEG 2000
6. Temporal: *frame dropping*, *frame averaging*, dan *frame swapping*

### B. *Singular Value Decomposition*

SVD adalah faktorisasi suatu matriks menjadi tiga matriks [9]. Suatu matriks  $A$  pada SVD akan terdiri dari: orthonormal vektor eigen  $AA^T$ , matriks transpose berisi orthonormal vektor  $A^T A$ , dan matriks diagonal berisi akar kuadrat dari nilai eigen  $A^T A$ . SVD digunakan untuk mendapatkan informasi dari suatu informasi. Rumus matematika untuk SVD dapat dilihat pada Persamaan (2).

$$A = U \cdot W \cdot V^T \quad (2)$$

dengan  $U$  adalah orthonormal vektor eigen  $AA^T$ ,  $W$  adalah matriks diagonal akar kuadrat dari nilai eigen  $A^T A$ , dan  $V^T$  adalah matriks transpose berisi orthonormal vektor  $A^T A$

Matriks  $U$  adalah matriks  $m \times m$ . Ketika matriks  $U$  melakukan perkalian matriks dengan  $U^T$  maka akan menghasilkan matriks identitas  $m \times m$ . Matriks  $W$  adalah matriks  $m \times n$ . Matriks  $V^T$  adalah matriks  $n \times n$ . Ketika matriks  $V^T$  melakukan perkalian matriks dengan  $V$  maka akan menghasilkan matriks identitas  $n \times n$ . Pada proses *watermarking*, matriks  $W$  digunakan sebagai tempat penanaman watermark karena perubahan nilai pada matriks  $W$  kasat mata [9].

### C. *Evaluasi*

Metode evaluasi pada penelitian ini digunakan untuk mengukur kualitas watermark dengan membandingkan watermark awal dengan watermark yang diekstrak dari video. Terdapat dua metrik yang digunakan, yaitu PSNR dan SSIM.

### 1) Peak Signal-to-Noise Ratio

PSNR adalah metrik yang umumnya digunakan untuk mengukur kualitas kompresi gambar [12]. PSNR membandingkan antara kekuatan sinyal dengan tingkat *noise* yang ada di dalam gambar tersebut. Semakin tinggi nilai PSNR, semakin baik kualitasnya. PSNR dihitung dengan menggunakan nilai logaritma jumlah maksimal piksel kuadrat dibagi dengan *mean squared error* (MSE). MSE adalah nilai error kuadrat rata-rata antara gambar asli dengan gambar *output*. Rumus matematika untuk PSNR dapat dilihat pada Persamaan (3). Rumus matematika untuk MSE dapat dilihat pada Persamaan (4).

$$PSNR = 10 \cdot \log_{10} \frac{MAX_I^2}{MSE} \quad (3)$$

$$MSE = \frac{1}{n} \sum_{n=1}^n (y - \hat{y})^2 \quad (4)$$

dengan  $MAX_I$  adalah jumlah maksimal piksel,  $n$  adalah jumlah data,  $y$  adalah target, dan  $\hat{y}$  adalah prediksi.

### 2) Structural Similarity Index Measure

SSIM adalah metrik yang digunakan untuk mengukur kesamaan struktural antara dua gambar [12]. SSIM terdiri dari tiga fungsi perbandingan yaitu: pencahayaan, kontras, dan struktur. Semakin tinggi nilai SSIM, maka semakin mirip kedua gambar tersebut. Rumus matematika untuk SSIM dapat dilihat pada Persamaan (5).

$$SSIM(x, y) = \frac{(2\mu_x\mu_y + c_1)(2\sigma_{xy} + c_2)}{(\mu_x^2 + \mu_y^2 + c_1)(\sigma_x^2 + \sigma_y^2 + c_2)} \quad (5)$$

dengan  $\mu$  adalah rata-rata dan  $\sigma$  adalah standar deviasi.

## III. ANALISIS DAN PERANCANGAN

### 1) Analisis Masalah

Media sosial adalah platform yang dapat digunakan untuk menyebarkan konten berupa gambar, video, dan musik. Konten yang disebarakan dapat memiliki hak cipta yang harus dihormati. Oleh karena itu, diperlukan suatu sistem yang mampu untuk mendeteksi konten yang memiliki hak cipta untuk membantu proses perlindungan hak cipta. Salah satu cara yang paling efektif digunakan adalah dengan menanamkan watermark pada konten sehingga dapat dengan mudah dideteksi oleh sistem. Watermark dapat ditanamkan secara terlihat maupun tak terlihat. Watermark yang terlihat memiliki kelemahan berupa merusak kualitas konten tersebut. Watermark yang tidak terlihat harus memiliki karakteristik *robust* yaitu ketahanan terhadap serangan yang bertujuan untuk mencegah pendeteksian watermark tersebut. Serangan yang digunakan dapat berupa penambahan *filter*, penambahan *noise*, dan *compression*. Cara untuk mengantisipasi serangan-serangan tersebut adalah dengan melakukan penanaman watermark pada domain spasial sehingga tahan terhadap perubahan.

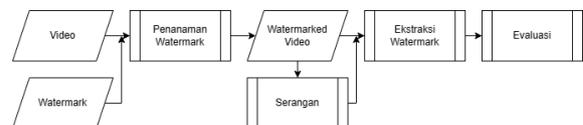
### 2) Gambaran Umum *Video watermarking*

Sistem *Video watermarking* terdiri dari algoritma penanaman watermark, algoritma ekstraksi watermark, algoritma serangan watermark, dan metode evaluasi.

Algoritma penanaman watermark memecah video menjadi beberapa *frame*, dan seluruh *frame* untuk melalui proses DWT untuk mendapatkan domain frekuensi gambar. Proses selanjutnya adalah SVD pada *channel* warna RGB untuk menyembunyikan watermark. Pada proses penanaman watermark, hasil nilai singular *frame* akan ditambahkan dengan nilai singular watermark. Setelah proses penanaman watermark selesai, akan dilakukan proses Inverse SVD dan Inverse DWT untuk mendapatkan *frame* yang mengandung watermark. *Frame* yang mengandung watermark akan disusun dengan *frame* lain untuk menghasilkan video sebagai *output*. Proses ekstraksi watermark dilaksanakan dengan metode yang sama dengan proses penanaman watermark namun hasil nilai singular *frame* akan dikurangi dengan nilai singular watermark. Setelah proses ekstraksi watermark selesai, akan didapatkan watermark awal. Proses ekstraksi akan diuji dengan menggunakan *input* hasil serangan berupa *noise*, *filter*, *trim*, dan *compression*. Kinerja algoritma penanaman maupun ekstraksi watermark akan diukur dengan menggunakan waktu komputasi, sedangkan kualitas watermark hasil ekstraksi akan diukur dengan menggunakan metrik PSNR dan SSIM.

### 3) Perancangan Metode

Implementasi sistem *watermarking* video terdiri dari beberapa subproses. Subproses pertama adalah penanaman watermark yang menerima *input* berupa video dan watermark, menghasilkan video yang mengandung watermark. Video tersebut lalu melalui eksperimen serangan *noise*, *filter*, dan *compression*. Jenis *noise* yang digunakan adalah *noise* acak, jenis *filter* yang digunakan adalah *gaussian filter*, dan jenis *compression* yang digunakan adalah JPEG. Ketiga metode serangan tersebut dipilih karena ketiga serangan tersebut umum digunakan pada media sosial. Subproses selanjutnya menerima *input* berupa video yang mengandung watermark awal dan video hasil serangan lalu mencoba untuk mengekstrak watermark dari kedua *input* tersebut. Langkah terakhir adalah evaluasi PSNR dan SSIM yang membandingkan watermark awal dengan watermark hasil ekstraksi untuk mengukur kualitas dan ketahanan metode watermark terhadap serangan.

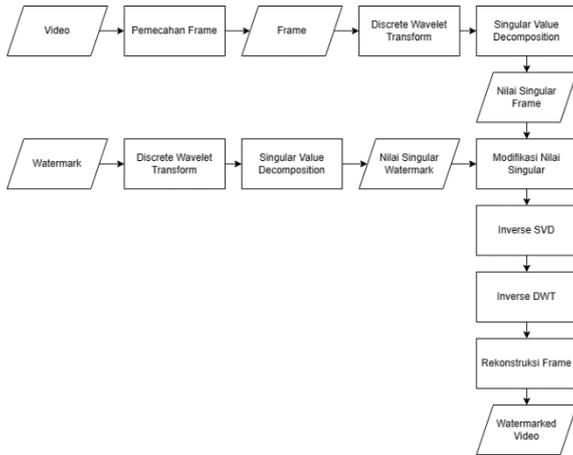


Gambar 1. Alur sistem

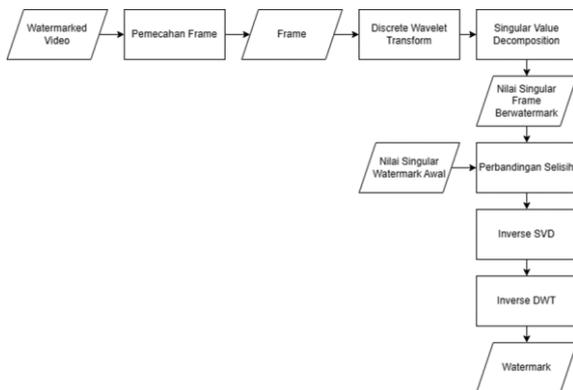
Metode penanaman watermark pada awalnya menerima *input* berupa video, lalu memecah video tersebut menjadi urutan gambar atau *frame*. seluruh *frame* akan melalui proses DWT. Hasil proses DWT adalah HH *subband* yang diproses menggunakan SVD pada channel warna RGB untuk menyembunyikan watermark. Proses SVD menghasilkan matriks  $U$ ,  $W$ , dan  $V^T$ , dengan matriks  $W$  sebagai matriks singular digunakan untuk mengandung nilai singular watermark. Matriks  $U$ , matriks  $W$  yang telah dimodifikasi, dan matriks  $V^T$  lalu akan melalui proses Inverse SVD dan Inverse DWT untuk mendapatkan *frame* yang mengandung watermark. Watermark yang digunakan adalah gambar biner logo ITB dengan latar belakang putih,

dalam bentuk *file png*. *Frame* yang telah mengandung watermark disusun kembali untuk menghasilkan video.

Metode ekstraksi watermark diawali dengan memecah kembali video menjadi *frame*, lalu memproses *frame* tersebut untuk mendapatkan bagian yang telah dimodifikasi pada proses penanaman watermark yaitu *subband HH*. Proses selanjutnya adalah mendapatkan nilai singular dengan menggunakan SVD lalu membandingkan selisih nilai singular awal dengan nilai singular yang telah dimodifikasi. Hasil perbandingan tersebut lalu melalui tahap Inverse SVD dan Inverse DWT untuk mendapatkan watermark.



Gambar 2. Alur metode penanaman watermark



Gambar 3. Alur metode ekstraksi watermark

#### IV. EVALUASI

##### 1) Deskripsi Dataset

Data yang digunakan pada penelitian ini adalah sebagian dari *dataset* TikTok Trending Videos yang berasal dari Kaggle. Data yang digunakan terdiri dari lima video berwarna yang memiliki dimensi  $576 \times 1024$ , 30 FPS, dan ekstensi \*.mp4. Informasi terkait dengan data yang digunakan pada penelitian ini dapat dilihat pada Tabel 1.

TABEL 1. INFORMASI DATASET

Nama File	Ukuran (KB)	Bitrate (kbps)	Durasi (s)
archer	327	275	8
bed	701	632	7
face	514	520	7
gym	547	325	11
race	827	579	9

##### 2) Hasil Eksperimen

Hasil eksperimen kualitas watermark terdiri dari nama *file* beserta dengan PSNR dan SSIM pada skenario serangan yaitu: tanpa serangan, *filter*, *noise*, dan *compression*. Hasil evaluasi PSNR dapat dilihat pada Tabel 2. Hasil evaluasi SSIM dapat dilihat pada Tabel 3.

TABEL 2. HASIL EVALUASI PSNR

Nama File	Skenario serangan			
	TS	F	N	C
archer	16,234	16,699	16,238	16,179
bed	16,589	16,707	16,585	16,593
face	16,412	16,714	16,407	16,4
gym	16,392	16,711	16,424	16,49
race	16,675	16,693	16,685	16,685

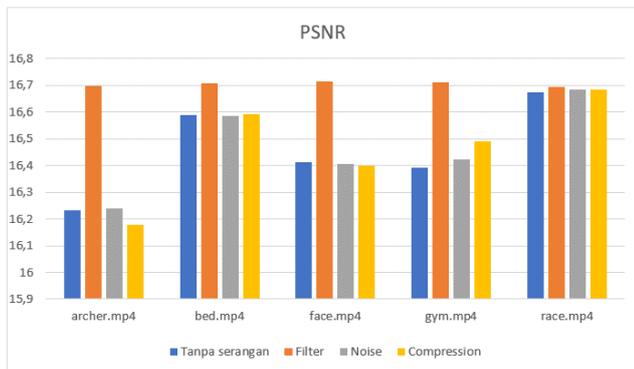
TS = Tanpa serangan, F = Filter, N = Noise, C = Compression

TABEL 3. HASIL EVALUASI SSIM

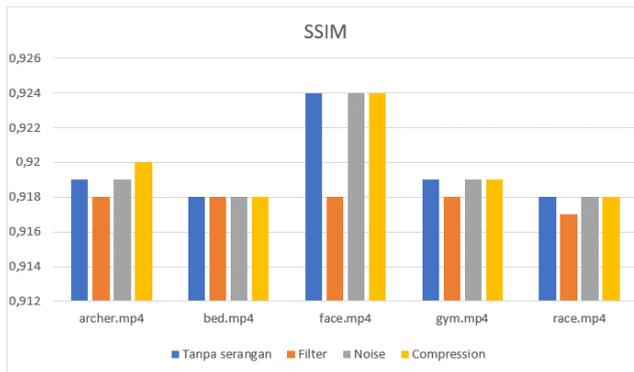
Nama File	Skenario serangan			
	TS	F	N	C
archer	0,919	0,918	0,919	0,92
bed	0,918	0,918	0,918	0,918
face	0,924	0,918	0,924	0,924
gym	0,919	0,918	0,919	0,919
race	0,918	0,917	0,918	0,918

TS = Tanpa serangan, F = Filter, N = Noise, C = Compression

Hasil eksperimen menunjukkan bahwa kualitas watermark relatif rendah dengan nilai rata-rata PSNR 16,46 db untuk skenario tanpa serangan, 16,704 db untuk skenario serangan *filter*, 10,467 db untuk skenario serangan *noise*, dan *compression*. Namun, jika dilihat dari nilai SSIM kualitas watermark tergolong baik dengan nilai rata-rata SSIM 0,918 untuk seluruh skenario serangan selain serangan *filter* dengan nilai SSIM 0,917. Selain itu, dapat dilihat bahwa *file* archer.mp4 memiliki nilai PSNR dan SSIM yang paling rendah dibandingkan dengan video lain pada setiap skenario. Hal ini dikarenakan video tersebut memiliki *bitrate* yang rendah yaitu 275 kbps, dibandingkan dengan video lain yang memiliki *bitrate* sekitar 600 kbps. *File* race.mp4 memiliki PSNR dan SSIM tertinggi karena video tersebut memiliki background berwarna hitam sehingga memiliki informasi yang lebih sedikit dibandingkan dengan video lain. Perbandingan hasil nilai PSNR dapat dilihat pada Gambar 4. Perbandingan hasil nilai SSIM dapat dilihat pada Gambar 5.



Gambar 4. Perbandingan hasil nilai PSNR



Gambar 5. Perbandingan hasil nilai SSIM

Hasil eksperimen kinerja algoritme terdiri dari nama *file* berserta dengan waktu komputasi penanaman watermark serta ekstraksi watermark yang dibagi sesuai dengan skenario serangan yaitu: tanpa serangan, *filter*, *noise*, dan *compression*. Hasil eksperimen kinerja algoritma dapat dilihat pada Tabel 4.

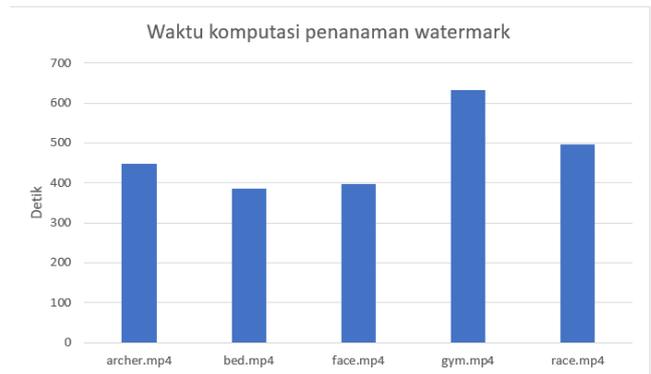
TABEL 4. HASIL EVALUASI WAKTU KOMPUTASI

Nama File	Waktu komputasi (s)				
	P	E			
		TS	F	N	C
archer	447,554	7,051	7,308	7,366	7,486
bed	386,459	7,635	7,489	7,557	7,513
face	397,568	7,715	7,599	7,498	7,495
gym	632,504	7,701	7,52	7,426	7,545
race	495,86	7,883	7,023	7,581	7,624

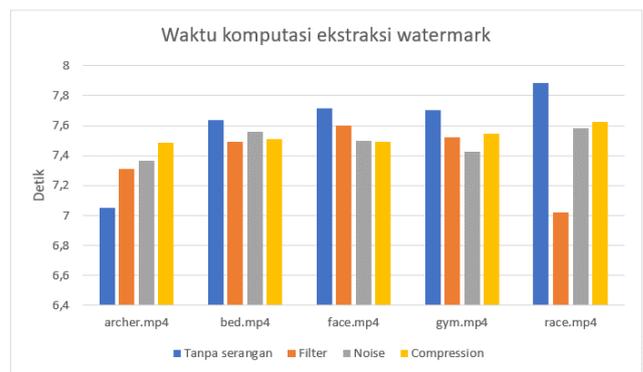
P = Penanaman watermark, E = Ekstraksi watermark, TS = Tanpa serangan, F = Filter, N = Noise, C = Compression

Algoritme penanaman berjalan dengan rata-rata waktu 7 menit 54 detik. Kinerja algoritme ekstraksi watermark relatif cepat dengan waktu rata-rata yaitu 7,597 detik untuk ekstraksi video tanpa serangan, 7,387 detik untuk ekstraksi video telah mengalami serangan *filter*, 7,485 detik untuk ekstraksi video telah mengalami serangan *noise*, dan 7,532 detik untuk ekstraksi video telah mengalami serangan *compression*. Waktu komputasi algoritme penanaman watermark memiliki korelasi dengan durasi video. *File* gym.mp4 yang membutuhkan waktu terlama untuk menyelesaikan proses penanaman watermark memiliki durasi video terlama yaitu 10 menit 32 detik. Waktu komputasi proses ekstraksi watermark tidak memiliki perubahan yang besar pada skenario-skenario yang telah dijalankan. Perbandingan waktu komputasi penanaman watermark dapat dilihat pada

Gambar 6. Perbandingan waktu komputasi ekstraksi watermark dapat dilihat pada Gambar 7.



Gambar 6. Perbandingan waktu komputasi penanaman watermark



Gambar 7. Perbandingan waktu komputasi ekstraksi watermark

## V. KESIMPULAN

Hasil eksperimen pada penelitian ini menemukan bahwa proses ekstraksi watermark algoritme SVD memiliki kualitas yang relatif rendah dengan nilai rata-rata PSNR 16,5 db. Hal ini dikarenakan kualitas watermark memiliki korelasi dengan *bitrate* video yang digunakan. Video yang digunakan pada penelitian ini memiliki *bitrate* yang terbatas yaitu sekitar 300 hingga 600 kbps. Penelitian ini juga mendapatkan bahwa algoritme SVD memiliki ketahanan terhadap serangan *noise*, *filter*, dan *compression*. Selain itu, hasil eksperimen menemukan bahwa algoritme SVD memiliki kinerja yang relatif baik dengan waktu komputasi yang cepat dengan waktu rata-rata 7 menit 54 detik. Kinerja algoritma ekstraksi watermark relatif cepat dengan waktu rata-rata yaitu 7,597 detik untuk ekstraksi video tanpa serangan, 7,387 detik untuk ekstraksi video telah mengalami serangan *filter*, 7,485 detik untuk ekstraksi video telah mengalami serangan *noise*, dan 7,532 detik untuk ekstraksi video telah mengalami serangan *compression*. Waktu komputasi algoritme penanaman watermark memiliki korelasi dengan durasi video. Waktu komputasi algoritme penanaman watermark memiliki korelasi dengan durasi video.

## DAFTAR PUSTAKA

- [1] J. H. Kietzmann, K. Hermkens, I. P. McCarthy, dan B. S. Silvestre, "Social media? Get serious! Understanding the functional building blocks of social media," *Bus Horiz*, vol. 54, no. 3, hlm. 241–251, Mei 2011, doi: 10.1016/J.BUSHOR.2011.01.005.
- [2] S. Dixon, "Social Media Statistics & Facts | Statista," 21 Juni 2022. <https://www.statista.com/topics/1164/social-networks/> (diakses 10 April 2023).
- [3] H. Nurhayati, "Social media in Indonesia - statistics & facts | Statista," 26 Januari 2023. <https://www.statista.com/topics/8306/social-media-in-indonesia/#topicOverview> (diakses 10 April 2023).
- [4] P. Wayner, "Disappearing Cryptography: Information Hiding: Steganography and Watermarking," *Disappearing Cryptography: Information Hiding: Steganography and Watermarking*, hlm. 1–439, Des 2008, doi: 10.1016/C2009-0-19136-5.
- [5] R. Singh *dkk.*, "From classical to soft computing based watermarking techniques: A comprehensive review," *Future Generation Computer Systems*, vol. 141, hlm. 738–754, Apr 2023, doi: 10.1016/J.FUTURE.2022.12.015.
- [6] R. Singh, L. I. Izhar, I. Elamvazuthi, A. Ashok, S. Aole, dan N. Sharma, "Efficient Watermarking Method Based on Maximum Entropy Blocks Selection in Frequency Domain for Color Images," *IEEE Access*, vol. 10, hlm. 52712–52723, 2022, doi: 10.1109/ACCESS.2022.3174964.
- [7] H. Wang, Z. Yuan, S. Chen, dan Q. Su, "Embedding color watermark image to color host image based on 2D-DCT," *Optik (Stuttg)*, vol. 274, hlm. 170585, Mar 2023, doi: 10.1016/J.IJLEO.2023.170585.
- [8] M. E. Moghaddam dan N. Nemati, "A robust color image watermarking technique using modified Imperialist Competitive Algorithm," *Forensic Sci Int*, vol. 233, no. 1–3, hlm. 193–200, Des 2013, doi: 10.1016/J.FORSCIINT.2013.09.005.
- [9] H. Zhang, C. Wang, dan X. Zhou, "A robust image watermarking scheme based on SVD in the spatial domain," *Future Internet*, vol. 9, no. 3, Agu 2017, doi: 10.3390/FI9030045.
- [10] R. O. Preda dan D. N. Vizireanu, "A robust digital watermarking scheme for video copyright protection in the wavelet domain," *Measurement*, vol. 43, no. 10, hlm. 1720–1726, Des 2010, doi: 10.1016/J.MEASUREMENT.2010.07.009.
- [11] K. M. Singh, "A robust rotation resilient video watermarking scheme based on the SIFT," *Multimed Tools Appl*, vol. 77, no. 13, hlm. 16419–16444, Jul 2018, doi: 10.1007/S11042-017-5213-9.
- [12] A. Horé dan D. Ziou, "Image quality metrics: PSNR vs. SSIM," *Proceedings - International Conference on Pattern Recognition*, hlm. 2366–2369, 2010, doi: 10.1109/ICPR.2010.579.