JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2068-2075
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.520

Analisis Performa Kecepatan Enkripsi File Video Menggunakan Algoritma DSA dan Twofish Berbasis Web

Rehansyah Akbar Nasution[1], Tommy[2*]

[1,2]Fakultas Teknik dan Komputer, Teknik Informatika, Universitas Harapan Medan, Medan, Indonesia
Email: [1*]abauakbar014@gmail.com, [2*]tomshirakawa@gmail.com
(*Email Corresponding Author: tomshirakawa@gmail.com)
Received: 29 Juli 2025 | Revision: 8 Agustus 2025 | Accepted: 21 Januari 2026

Abstrak

Keamanan data merupakan aspek krusial dalam pengelolaan dan distribusi file digital, terutama file video yang berukuran besar dan berpotensi mengandung informasi sensitif. Dalam konteks ini, diperlukan pendekatan kriptografi yang tidak hanya menjamin kerahasiaan data, tetapi juga memastikan integritas dan keasliannya. Penelitian ini bertujuan untuk menganalisis performa kombinasi algoritma Twofish dan Digital Signature Algorithm (DSA) dalam proses enkripsi dan dekripsi file video pada aplikasi berbasis web. Algoritma Twofish, sebagai metode simetris, dipilih karena kemampuannya dalam mengolah data berukuran besar secara cepat dan efisien. Sementara itu, DSA digunakan sebagai algoritma asimetris untuk menghasilkan tanda tangan digital yang menjamin validitas dan integritas file. Aplikasi yang dikembangkan memungkinkan pengguna mengunggah video, melakukan enkripsi dengan kunci acak menggunakan Twofish, serta menghasilkan tanda tangan digital dengan DSA. Pengujian dilakukan terhadap lima file video dengan ukuran bervariasi, dari 4,59 MB hingga 43,5 MB. Hasil menunjukkan bahwa seluruh proses enkripsi dan dekripsi berjalan sukses dan menghasilkan tanda tangan digital yang valid. Waktu enkripsi berkisar antara 8,88 detik hingga 01 menit 26,41 detik, sedangkan waktu dekripsi berkisar antara 8,28 detik hingga 01 menit 24,31 detik. Rata-rata waktu enkripsi tercatat 33,17 detik, sementara dekripsi rata-rata 32,61 detik. Selisih waktu antar proses relatif kecil, menandakan efisiensi algoritma Twofish dalam kedua arah operasi. Selain itu, waktu pemrosesan meningkat seiring bertambahnya ukuran file, namun tetap dalam batas wajar untuk aplikasi web. Secara keseluruhan, kombinasi Twofish dan DSA terbukti efektif dan efisien untuk meningkatkan keamanan file video berbasis web tanpa mengorbankan performa sistem.

Kata Kunci: *Twofish, Digital Signature Algorithm (DSA), enkripsi video, integritas data.*

Abstract

Data security is a crucial aspect in the management and distribution of digital files, particularly video files, which are typically large in size and may contain sensitive information. In this context, a cryptographic approach is required that not only ensures data confidentiality but also guarantees its integrity and authenticity. This study aims to analyze the performance of combining the Twofish algorithm and the Digital Signature Algorithm (DSA) in the encryption and decryption processes of video files within a web-based application. Twofish, a symmetric algorithm, was chosen for its high efficiency in processing large datasets, while DSA, an asymmetric algorithm, is used to generate digital signatures that verify the validity and integrity of the files. The developed application allows users to upload video files, encrypt them using randomly generated Twofish keys, and generate digital signatures using DSA. Testing was conducted on five video files with varying sizes, ranging from 4.59 MB to 43.5 MB. The results showed that all encryption and decryption processes were successfully completed, and all generated digital signatures were valid. Encryption times ranged from 8.88 seconds to 1 minute 26.41 seconds, while decryption times ranged from 8.28 seconds to 1 minute 24.31 seconds. The average encryption time was 33.17 seconds, and the average decryption time was 32.61 seconds. The small time differences between encryption and decryption indicate the efficiency of the Twofish algorithm in both directions. Furthermore, processing times increased with file size but remained within reasonable limits for web-based applications. Overall, the combination of Twofish and DSA has proven to be an effective and efficient solution for enhancing video file security on web platforms without compromising system performance.

Keywords: *Twofish, Digital Signature Algorithm (DSA), video encryption, data integrity*

1. PENDAHULUAN

Dalam era transformasi digital yang pesat, keamanan data menjadi salah satu aspek krusial yang harus diperhatikan dalam berbagai bentuk pertukaran informasi [1]. Salah satu jenis data yang paling sering digunakan dan dibagikan secara daring adalah file video. Video digunakan tidak hanya dalam bidang hiburan, tetapi juga dalam sektor pendidikan, komunikasi bisnis, hingga sistem keamanan. Seiring meningkatnya penggunaan file video dalam berbagai aktivitas daring, ancaman terhadap privasi dan integritas data juga semakin tinggi [2]. Maka dari itu, diperlukan strategi pengamanan yang efektif, salah satunya melalui enkripsi file.

File video memiliki karakteristik khusus yang membedakannya dari jenis data lain [3]. Ukurannya relatif besar, bersifat biner, dan memerlukan waktu pemrosesan yang signifikan jika akan diamankan melalui enkripsi. Oleh karena itu, pemilihan algoritma enkripsi yang tepat tidak hanya harus mempertimbangkan tingkat keamanan, tetapi juga efisiensi waktu dalam proses enkripsi dan dekripsi [4]. Apalagi jika sistem tersebut diimplementasikan dalam platform berbasis web, yang notabene memiliki keterbatasan sumber daya baik di sisi klien maupun server [5].

Algoritma kriptografi yang banyak digunakan umumnya terbagi menjadi dua jenis utama: simetris dan asimetris. Algoritma simetris menggunakan satu kunci yang sama untuk proses enkripsi dan dekripsi, sehingga lebih cepat dan cocok untuk mengamankan data berukuran besar. Sementara itu, algoritma asimetris menggunakan pasangan kunci

This Journal is licensed under a Creative Commons Attribution 4.0 International License.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2068-2075
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.520

publik dan privat, dan lebih unggul dalam hal otentikasi dan integritas data. Penggabungan kedua jenis algoritma dalam satu sistem disebut sebagai *hybrid cryptosystem* [6], dan telah terbukti mampu mengoptimalkan kekuatan masing-masing pendekatan.

Twofish merupakan salah satu algoritma enkripsi simetris yang dirancang untuk efisiensi tinggi dan fleksibilitas, serta mampu menangani data besar dengan performa yang baik [7]. Twofish dikenal dengan struktur kunci yang kompleks namun efisien, menjadikannya kandidat yang relevan dalam konteks enkripsi file video secara keseluruhan. Sementara itu, Digital Signature Algorithm (DSA) merupakan metode kriptografi asimetris yang berfungsi untuk memastikan bahwa file tidak dimodifikasi serta menjamin identitas pengirim melalui tanda tangan digital [8]. Dalam sistem hybrid, DSA berperan dalam memberikan keaslian (authenticity) dan integritas (integrity) atas file video yang telah dienkripsi menggunakan Twofish. Implementasi sistem keamanan seperti ini dalam aplikasi web menuntut perhatian lebih terhadap performa sistem, khususnya pada aspek kecepatan [9]. Web server yang menangani proses enkripsi dan dekripsi file video secara langsung harus mampu mengelola beban pemrosesan tanpa menyebabkan keterlambatan atau gangguan pada layanan pengguna. Oleh karena itu, pengujian performa, terutama dalam mengukur waktu enkripsi dan dekripsi terhadap file dengan ukuran besar, menjadi penting sebagai dasar validasi efisiensi algoritma yang digunakan [10].

Dalam penelitian ini, proses enkripsi dilakukan secara langsung terhadap file video dalam format MP4 dalam bentuk byte stream, bukan pada tingkat frame atau konten visualnya. Pendekatan ini memungkinkan penerapan algoritma enkripsi secara menyeluruh dan lebih praktis, serta relevan dengan skenario penggunaan sehari-hari seperti pengunggahan atau pengunduhan video melalui web [11]. Dengan demikian, penelitian ini tidak hanya mengevaluasi aspek keamanan, tetapi juga memperhatikan faktor performa sistem dalam skala implementasi nyata. Tujuan utama dari penelitian ini adalah untuk menganalisis kecepatan enkripsi dan dekripsi file video menggunakan algoritma Twofish dan DSA dalam konteks aplikasi web. Hasil dari analisis ini diharapkan dapat memberikan kontribusi terhadap pengembangan sistem keamanan data multimedia berbasis web yang efisien, aman, dan dapat diterapkan secara luas dalam berbagai kebutuhan digital yang melibatkan distribusi video [12].

2. METODOLOGI PENELITIAN

2.1. DSA

Digital Signature Algorithm adalah salah satu metode yang digunakan untuk memastikan keaslian data, sehingga penerima dapat memverifikasi apakah data yang diterima adalah benar asli atau telah dipalsukan. Teknologi Digital Signature dilakukan dengan menggunakan sistem kriptografi kunci privat dan kunci publik. Dalam sistem ini, dibuat sepasang kunci, yaitu kunci privat dan kunci publik. Kunci privat disimpan oleh pemiliknya dan digunakan untuk menghasilkan tanda tangan digital, sedangkan kunci publik dapat dibagikan kepada siapa saja yang ingin memverifikasi keaslian tanda tangan digital pada suatu dokumen. Proses pembentukan dan verifikasi tanda tangan ini melibatkan teknik kriptografi seperti hashing.

Adapun beberapa parameter *Digital Signature Algorithm(DSA)*, yaitu sebagai berikut [13] :

1. p, adalah bilangan prima dengan panjang 1024 bit. Parameter p bersifat publik dan dapat digunakan bersama-sama oleh orang di dalam kelompok.
2. q, bilangan prima 160 bit, merupakan faktor dari p–1. Dengan kata lain, (p–1) mod q=0. Parameter qbersifat publik.
3. g= h(p-1)/qmod p, dimana h< p–1 sedemikian sehingga h(p-1)/qmod p> 1. Parameter gbersifat publik.
4. x, adalah bilangan bulat kurang dari q. Parameter xadalah kunci pribadi.
5. y =gxmod p, adalah kunci publik.f.m,pesan yang akan diberi tanda tangan.

Ada beberapa langkah dalam pembentukan *Digital Signature Algorithm*, yaitu [14] :

1. Membuat sepasang kunci:
   Pilih bilangan prima p dan q, dengan persamaan $(p-1)\ mod\ q = 0$
   $g = h(p-1)/q\ mod\ p$, dalam persamaan $1 < h < p-1$ dan $h(p-1)/q\ mod\ p > 1$
   $x < q$ = merupakan kunci privat
   $y = gx\ mod\ p$ = kunci publik
2. Proses pembuatan tanda tangan
   $k < q$ = bilangan acak
   $r = (gk\ mod\ p)\ mod\ q$
   $s = (k-1(H(m) + x * r))mod\ q$. $k-1$ yaitu invers $k\ mod\ q$
   (r, s): tanda tangan digital
3. Proses pembuktian tanda tangan (verifikasi)
   $w = s-1\ mod\ q$
   $u1 = ((m) * w)\ mod\ q$
   $u2 = (r * w)\ mod\ q$
   $v = ((gu1 * yu2)\ mod\ p)\ mod\ q$

   Jika $v = r$, maka tanda tangan terbukti asli.

Copyright © 2026 **Author**, Page 2069
This Journal is licensed under a Creative Commons Attribution 4.0 International License.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2068-2075
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.520

2.2. Twofish

Twofish adalah algoritma kriptografi simetris berbasis blok cipher yang menggunakan blok input sebesar 128 bit, dan mendukung panjang kunci sebesar 128 bit, 192 bit, atau 256 bit. Pada implementasi algoritma *Twofish*, terdapat beberapa hal yang harus diperhatikan, antara lain [15] :

1. Bit masukan sebanyak 128 bit akan dibagi menjadi empat bagian masing-masing sebesar 32 bit menggunakan konvensi little-endian. Dua bagian bit akan menjadi bagian kanan, dua bagian bit lainnya akan menjadi bagian kiri.
2. Bit input akan di-XOR terlebih dahulu dengan empat bagian kunci, atau dengan kata lain mengalami proses whitening. R0,i = Pi ⊕_Ki i = 0, ..., 3 Dimana K adalah kunci, Ki berarti sub kunci yang ke-i.
3. Seperti telah dibahas diatas, algoritma *Twofish* menggunakan struktur jaringan Feistel. Jaringan Feistel yang digunakan oleh *Twofish* terdiri dari 16 iterasi. Fungsi f dari *Twofish* terdiri dari beberapa tahap, yaitu:
   a. Fungsi g, yang terdiri dari empat s-box dan matriks MDS
   b. PHT (pseudo-hadamard trans*Form*/ perubahan pseudo hadamard)
   Penambahan hasil PHT dengan kunci.

2.3. File Video

Video merupakan teknologi yang digunakan untuk memproses sinyal elektronik guna merepresentasikan gambar bergerak. Secara umum, video terdiri dari rangkaian gambar bergerak yang dihasilkan melalui perekaman dengan kamera atau melalui animasi komputer. Awalnya, informasi video disimpan dalam format analog, yaitu dalam bentuk sinyal gelombang kontinu yang merepresentasikan perubahan warna dan tingkat kecerahan dari gambar yang direkam [16]. File video adalah jenis data yang mudah diakses oleh berbagai pihak. Namun, kemudahan akses ini menjadikan video rentan terhadap pencurian dan serangan oleh pihak yang tidak berwenang. Untuk mencegah hal tersebut, diperlukan penerapan sistem *enkripsi* guna melindungi file video agar tidak disalahgunakan atau diakses oleh pihak yang tidak memiliki izin dan melihat bagaimana performa kecepatan proses *enkripsi* dan *dekripsi* file video.

3. HASIL DAN PEMBAHASAN

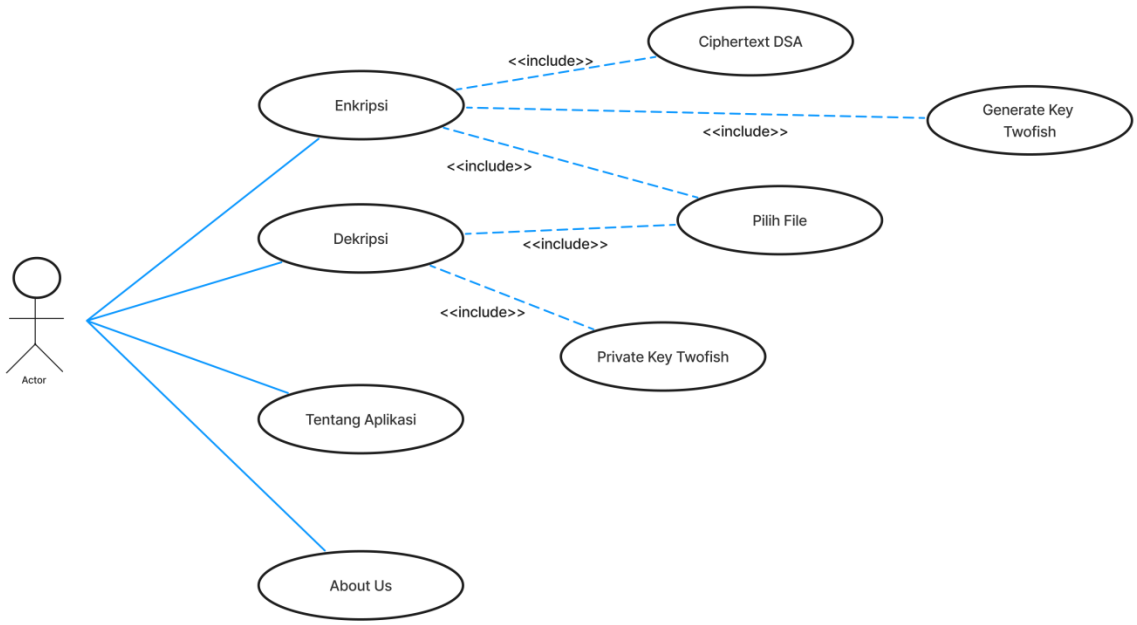
Penelitian ini menggunakan pendekatan kuantitatif dengan metode eksperimen untuk menganalisis performa kecepatan proses enkripsi file video menggunakan kombinasi algoritma Twofish dan DSA. Fokus utama penelitian adalah mengukur dan membandingkan waktu yang dibutuhkan dalam proses enkripsi dan dekripsi file video berukuran besar pada lingkungan aplikasi berbasis web. Penelitian ini dilakukan secara terstruktur melalui beberapa tahapan, sebagaimana dijelaskan berikut.

3.1. Desain Sistem

Penelitian ini menerapkan sistem keamanan berbasis *hybrid cryptosystem*, yaitu menggabungkan algoritma simetris (Twofish) untuk enkripsi data dan algoritma asimetris (DSA) untuk pembuatan serta verifikasi tanda tangan digital. File video dalam format MP4 akan dienkripsi secara utuh dalam bentuk byte stream menggunakan kunci acak yang dihasilkan oleh Twofish. Selanjutnya, file hasil enkripsi akan disertai dengan tanda tangan digital yang dibuat menggunakan DSA berdasarkan konten asli file tersebut.

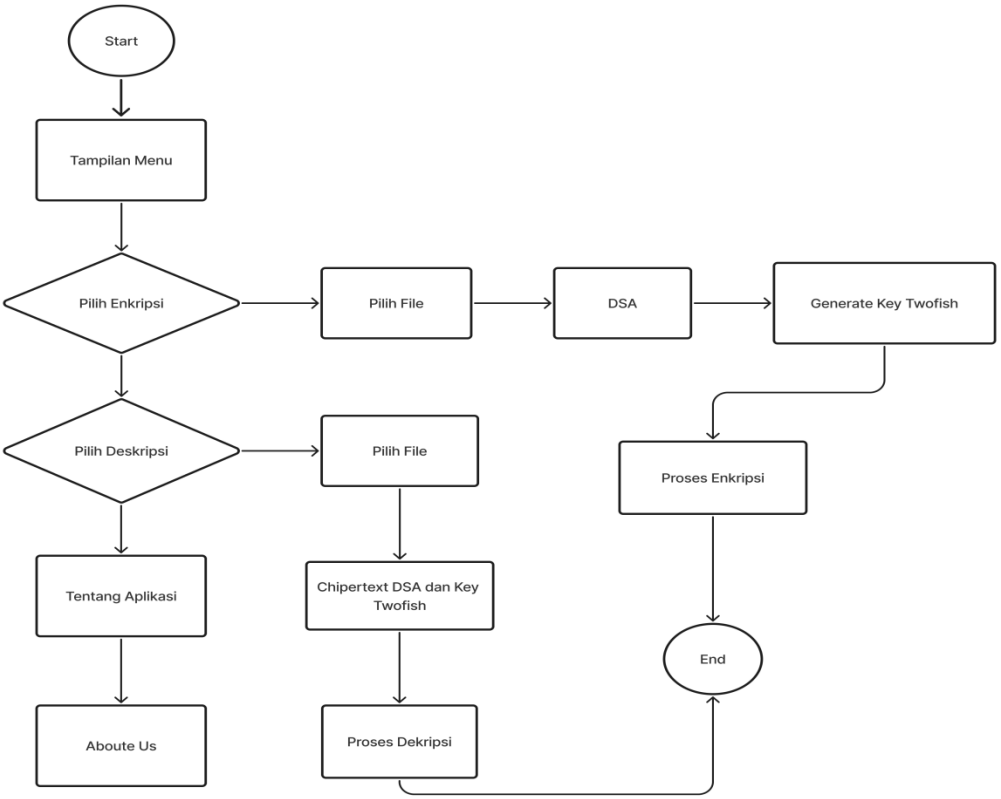
This Journal is licensed under a Creative Commons Attribution 4.0 International License.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2068-2075
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.520



Gambar 1. Use Case Enkripsi dan Dekripsi

Proses enkripsi dan dekripsi file video pada aplikasi web ini dimulai saat pengguna mengakses halaman utama dan memilih menu enkripsi untuk mengunggah file video serta memasukkan kunci awal berbasis hashing DSA. Sistem kemudian membangkitkan sepasang kunci Twofish (publik dan privat), di mana kunci privat akan diunduh oleh pengguna untuk keperluan dekripsi. Setelah menekan tombol submit, sistem membagi file video menjadi blok-blok kecil yang masing-masing dienkripsi secara iteratif menggunakan kunci publik Twofish dan dilengkapi tanda tangan digital berupa ciphertext DSA. Hasil enkripsi akan diunduh secara otomatis. Untuk dekripsi, pengguna mengunggah file terenkripsi, ciphertext, dan kunci privat, lalu sistem memproses pembagian blok, dekripsi menggunakan kunci privat, serta verifikasi dengan ciphertext DSA.



Gambar 2. *Flowchart* Sistem

Copyright © 2026 **Author**, Page 2071
This Journal is licensed under a Creative Commons Attribution 4.0 International License.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2068-2075
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.520

Diagram alir sistem seperti yang terlihat pada gambar 2 menggambarkan alur proses enkripsi dan dekripsi file video dalam aplikasi web menggunakan algoritma Twofish dan DSA. Proses dimulai ketika pengguna mengakses aplikasi dan memilih salah satu dari dua opsi, yaitu enkripsi atau dekripsi. Jika memilih enkripsi, pengguna mengunggah file video, memasukkan kunci awal DSA, lalu sistem membangkitkan sepasang kunci Twofish dan mengunduh kunci privat ke pengguna. Setelah itu, file dibagi menjadi blok-blok kecil dan dienkripsi secara iteratif menggunakan kunci publik Twofish serta dilengkapi tanda tangan digital DSA, hingga sistem menghasilkan dan mengunduh file terenkripsi. Untuk dekripsi, pengguna mengunggah file terenkripsi, file ciphertext DSA, dan kunci privat. Sistem kemudian membagi ulang file, mendekripsi tiap blok menggunakan kunci privat, serta memverifikasi integritasnya dengan DSA. Jika berhasil, file video asli diunduh secara otomatis, menandakan proses dekripsi selesai.

3.2. Lingkungan Pengujian

Implementasi dilakukan dalam lingkungan berbasis web menggunakan teknologi PHP dan JavaScript untuk sisi klien dan server. Eksperimen dijalankan pada server lokal dengan spesifikasi sebagai berikut :

a. *Frontend: HTML, CSS, JavaScript*
b. *Backend: PHP / Python*
c. Algoritma *Kriptografi DSA*: Untuk pengamanan melalui tanda tangan digital (meski bukan untuk *enkripsi* utama, bisa digunakan untuk otentikasi data).
d. Algoritma *Kriptografi Twofish*: Untuk *enkripsi simetris* file video.
e. Server: *Web* server lokal atau berbasis *cloud (XAMPP)*

3.3. Pengukuran Performa

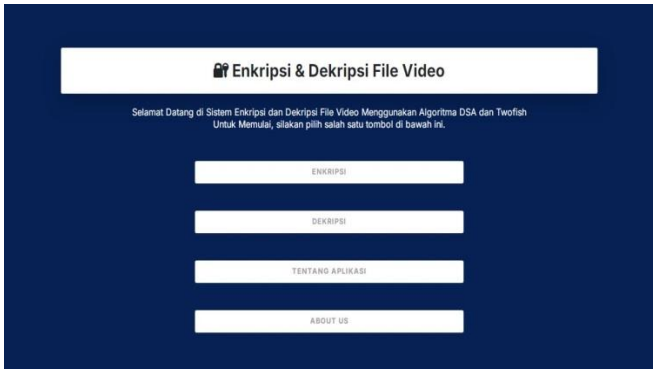
Evaluasi kecepatan sistem dilakukan untuk menilai performa dari proses *enkripsi* dan *dekripsi* file video menggunakan algoritma *Twofish* dan *DSA* dalam lingkungan *web*. Tujuan evaluasi ini adalah untuk mengukur efisiensi waktu proses serta dampaknya terhadap pengalaman pengguna. Evaluasi kecepatan didasarkan pada tiga parameter utama:

1. Waktu *Enkripsi*
   Waktu yang dibutuhkan sistem untuk mengubah file video asli menjadi file ter*enkripsi*.
2. Waktu *Dekripsi*
   Waktu yang diperlukan untuk mengembalikan file ter*enkripsi* menjadi bentuk aslinya.
3. Ukuran File
   Sejauh mana ukuran file video berubah sebelum dan sesudah di*enkripsi*.

3.4. Validasi Hasil

Untuk memastikan keakuratan dan integritas hasil, proses dekripsi akan dilakukan untuk setiap file terenkripsi, dan hasilnya dibandingkan dengan file asli. Jika file hasil dekripsi identik dengan file asli dan tanda tangan digital berhasil diverifikasi, maka proses dianggap valid. Jika terjadi perbedaan atau kegagalan verifikasi, maka sistem dianggap gagal dalam menjaga integritas data.

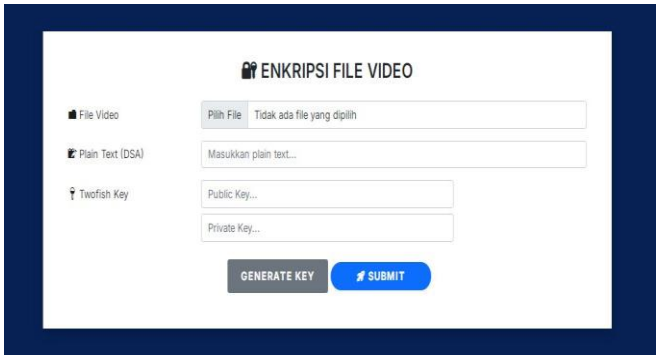
Aplikasi yang dikembangkan memiliki antarmuka berbasis web yang dirancang untuk memudahkan pengguna dalam melakukan proses unggah file, enkripsi, dan dekripsi secara langsung melalui browser. Implementasi difokuskan pada pengujian fungsionalitas sistem, antarmuka pengguna, serta analisis terhadap performa kecepatan proses enkripsi dan dekripsi. Berikut ini ditampilkan beberapa tampilan antarmuka aplikasi yang mencerminkan alur interaksi pengguna dalam menjalankan sistem yang telah dibangun.



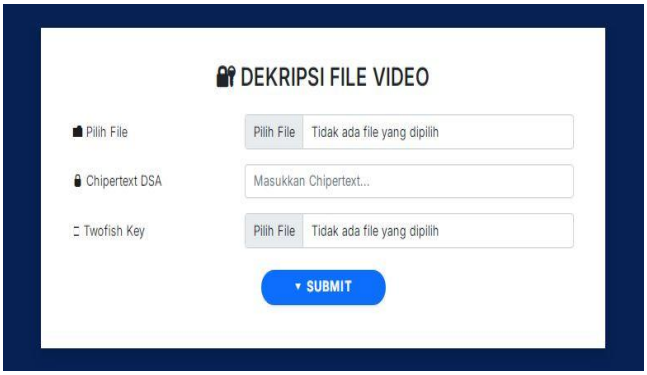
Gambar 3. Tampilan Sistem

Copyright © 2026 **Author**, Page 2072
This Journal is licensed under a Creative Commons Attribution 4.0 International License.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2068-2075
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.520



Gambar 4. Tampilan Sistem Enkripsi



Gambar 5. Tampilan Sistem Dekripsi

Setelah sistem berhasil diimplementasikan, dilakukan pengujian terhadap lima file video dengan ukuran dan durasi yang berbeda sebagai data uji. Pengujian ini bertujuan untuk mengevaluasi performa sistem dalam hal kecepatan proses enkripsi dan dekripsi menggunakan algoritma Twofish dan DSA. Setiap file video diproses melalui tahapan enkripsi dan dekripsi secara penuh dalam lingkungan aplikasi web, dengan waktu eksekusi dicatat secara manual pada masing-masing tahap. Hasil pengujian ini menjadi dasar dalam menganalisis sejauh mana efisiensi algoritma dapat dipertahankan terhadap file dengan kompleksitas dan ukuran yang bervariasi. Berikut adalah hasil lengkap dari pengujian yang telah dilakukan terhadap lima video uji tersebut.

Tabel 1. Tabel Software dan Hardware Pendukung

No	Nama File	Ukuran (MB)	Waktu Enkripsi (Detik)	Waktu Dekripsi (Detik)	Tanda Tangan Digital
1	Video1	4.59	08.88	08.28	Valid
2	Video2	9.54	11.54	10.33	Valid
3	Video3	17.7	24.33	23.67	Valid
4	Video4	23.6	36.67	34.45	Valid
5	Video5	43.5	01.26.41	01.24.31	Valid

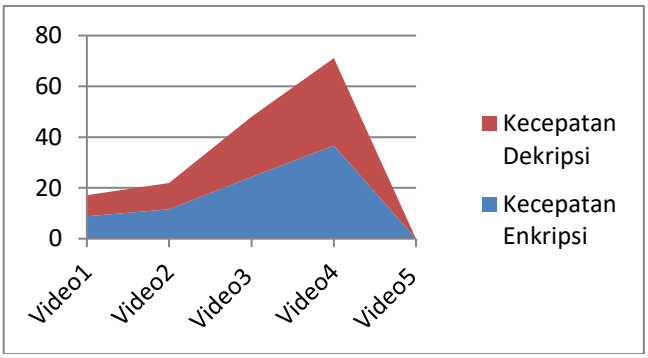
Dari tabel di atas, dapat dilihat bahwa setiap file video berhasil diproses melalui tahapan enkripsi dan dekripsi dengan status tanda tangan digital yang valid, menandakan bahwa integritas dan keaslian data tetap terjaga selama proses berlangsung. Waktu proses enkripsi dan dekripsi menunjukkan adanya peningkatan seiring bertambahnya ukuran file, dengan perbedaan waktu yang relatif seimbang antara kedua proses. Video dengan ukuran terbesar yaitu 43,5 MB membutuhkan waktu proses paling lama, baik saat enkripsi maupun dekripsi. Sementara itu, video dengan ukuran lebih kecil memerlukan waktu yang lebih singkat, menunjukkan bahwa performa sistem berbanding lurus dengan ukuran file yang diproses. Hasil ini menjadi dasar untuk analisis lebih lanjut terkait efisiensi algoritma yang digunakan dan pengaruh ukuran file terhadap performa sistem.

Hasil pengujian terhadap lima file video dengan ukuran yang bervariasi menunjukkan bahwa sistem enkripsi dan dekripsi berbasis web yang dibangun menggunakan algoritma Twofish dan DSA dapat berfungsi dengan baik. Seluruh file berhasil diproses secara utuh tanpa mengalami kerusakan data, dan setiap tanda tangan digital yang diverifikasi menunjukkan status valid. Hal ini mengindikasikan bahwa integritas dan keaslian file tetap terjaga selama proses berlangsung, yang merupakan fungsi utama dari penggunaan DSA dalam sistem ini.

Copyright © 2026 **Author**, Page 2073
This Journal is licensed under a Creative Commons Attribution 4.0 International License.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2068-2075
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.520

Dari sisi performa, waktu proses enkripsi dan dekripsi menunjukkan kecenderungan linier terhadap ukuran file. Semakin besar ukuran file video, semakin lama waktu yang dibutuhkan untuk menyelesaikan proses enkripsi maupun dekripsi. Pada file berukuran kecil seperti 4.59 MB dan 9.54 MB, waktu enkripsi berada di bawah 12 detik, sedangkan pada file terbesar (43.5 MB), waktu proses mencapai lebih dari satu menit. Meskipun demikian, perbedaan waktu antara proses enkripsi dan dekripsi cenderung tipis, menunjukkan efisiensi implementasi algoritma Twofish dalam menangani kedua proses secara seimbang.



Gambar 6. *Running Time* Enkripsi dan Dekripsi

Penggunaan Twofish sebagai algoritma simetris terbukti memberikan performa yang stabil dan cukup cepat dalam menangani file dengan ukuran besar, sesuai dengan karakteristik algoritma tersebut yang dioptimalkan untuk kecepatan dan keamanan. Sementara itu, DSA yang digunakan untuk membubuhkan tanda tangan digital tidak memberikan pengaruh signifikan terhadap waktu proses secara keseluruhan, karena hanya diterapkan pada hash dari file, bukan pada keseluruhan isi video.

4. KESIMPULAN

Berdasarkan hasil implementasi dan pengujian terhadap lima file video dengan ukuran bervariasi, dapat disimpulkan bahwa sistem enkripsi dan dekripsi file video berbasis web menggunakan algoritma Twofish dan DSA berjalan dengan baik dan stabil. Seluruh proses enkripsi dan dekripsi berhasil dilakukan tanpa kehilangan data, serta menghasilkan tanda tangan digital yang valid pada setiap file, sehingga menjamin integritas dan keaslian file video selama proses berlangsung. Penggunaan algoritma Twofish terbukti efektif dalam menangani file berukuran besar dengan waktu proses yang relatif efisien dan seimbang antara proses enkripsi dan dekripsi. Sementara itu, penerapan DSA sebagai tanda tangan digital tidak memberikan beban signifikan terhadap performa sistem, namun berperan penting dalam aspek keamanan, khususnya untuk verifikasi integritas file. Peningkatan ukuran file secara langsung berpengaruh terhadap durasi proses, menunjukkan bahwa performa sistem sensitif terhadap kompleksitas data. Namun demikian, sistem masih mampu menangani file dengan ukuran hingga puluhan megabyte dalam waktu yang dapat diterima untuk penggunaan web. Secara keseluruhan, sistem yang dibangun menunjukkan bahwa kombinasi algoritma Twofish dan DSA dapat diterapkan secara efektif untuk mengamankan file video dalam aplikasi berbasis web, baik dari sisi kecepatan, efisiensi, maupun kehandalan fungsi keamanan.

REFERENCES

[1] S. Oktaviani, F. Rizky, and I. Gunawan, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)," *J. Media Inform.*, vol. 4, no. 2, pp. 97–101, 2023, doi: 10.55338/jumin.v4i2.435.

[2] M. H. T. A. Thoriq, A. I. H. Asep, and P. N. S. Puspita, "Data Encryption Pada File Video Menggunakan Algoritma Blowfish Berbasis Android," *Informatics Digit. Expert*, vol. 4, no. 1, pp. 33–39, 2022, doi: 10.36423/index.v4i1.880.

[3] D. P. E. Andrian, D. H. Fudholi, and Y. Prayudi, "Karakteristik Metadata Pada Sharing File Di Media Sosial Untuk Mendukung Analisis Bukti Digital," *J. Ilm. SINUS*, vol. 19, no. 1, p. 13, 2021, doi: 10.30646/sinus.v19i1.494.

[4] Z. S. Gandhara, T. P. Satria, H. Saragih, and M. N. N. Abror, "Evaluasi Kinerja Algoritma Kriptografi dalam Pengamanan Video: Studi Perbandingan AES, DES dan Blowfish," *J. Ilm. Res. Student*, vol. 2, no. 2, pp. 917–923, 2025, doi: 10.61722/jirs.v2i2.5908.

[5] A. Aprizald, M. A. Hasan, and D. Setiawan, "Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi Dan Dekripsi Data," *JEKIN - J. Tek. Inform.*, vol. 2, no. 2, pp. 85–95, 2023, doi: 10.58794/jekin.v2i2.225.

[6] A. Takieldeen, S. H. Abd Elkhalik, A. S. Samra, M. A. Mohamed, and F. Khalifa, "A robust and hybrid cryptosystem for

This Journal is licensed under a Creative Commons Attribution 4.0 International License.

JURNAL KOMPUTER TEKNOLOGI INFORMASI SISTEM KOMPUTER
p-ISSN: 2962-3022 | e-ISSN: 2963-7104
Volume 4 No 3 Februari 2026
Hal: 2068-2075
http://ejurnal.lkpkaryaprima.id/index.php/juktisi
DOI: https://doi.org/10.62712/juktisi.v4i3.520

identity authentication," *Inf.*, vol. 12, no. 3, pp. 1–14, 2021, doi: 10.3390/info12030104.

[7] S. Praptodiyono, F. Muhammad, and D. Wiriyadinata, "Analysis security system performance MIPv6 in signaling process using AES and Twofish algorithms," *Tek. J. Sains dan Teknol.*, vol. 17, no. 2, p. 158, 2021, doi: 10.36055/tjst.v17i2.13069.

[8] M. R. Alfani, M. Furqan, and Y. R. Nasution, "Pengamanan Data Teks Menggunakan Metode[1] S. Oktaviani, F. Rizky, and I. Gunawan, "Analisis Keamanan Data Dengan Menggunakan Kriptografi Modern Algoritma Advance Encryption Standar (AES)," *J. Media Inform.*, vol. 4, no. 2, pp. 97–101, 2023, doi: 10.55338/jumin.v4i2.435.

[2] M. H. T. A. Thoriq, A. I. H. Asep, and P. N. S. Puspita, "Data Encryption Pada File Video Menggunakan Algoritma Blowfish Berbasis Android," *Informatics Digit. Expert*, vol. 4, no. 1, pp. 33–39, 2022, doi: 10.36423/index.v4i1.880.

[3] D. P. E. Andrian, D. H. Fudholi, and Y. Prayudi, "Karakteristik Metadata Pada Sharing File Di Media Sosial Untuk Mendukung Analisis Bukti Digital," *J. Ilm. SINUS*, vol. 19, no. 1, p. 13, 2021, doi: 10.30646/sinus.v19i1.494.

[4] Z. S. Gandhara, T. P. Satria, H. Saragih, and M. N. N. Abror, "Evaluasi Kinerja Algoritma Kriptografi dalam Pengamanan Video: Studi Perbandingan AES, DES dan Blowfish," *J. Ilm. Res. Student*, vol. 2, no. 2, pp. 917–923, 2025, doi: 10.61722/jirs.v2i2.5908.

[5] A. Aprizald, M. A. Hasan, and D. Setiawan, "Aplikasi Keamanan Data Berbasis Web Menggunakan Algoritma AES 128 Untuk Enkripsi Dan Dekripsi Data," *JEKIN - J. Tek. Inform.*, vol. 2, no. 2, pp. 85–95, 2023, doi: 10.58794/jekin.v2i2.225.

[6] A. Takieldeen, S. H. Abd Elkhalik, A. S. Samra, M. A. Mohamed, and F. Khalifa, "A robust and hybrid cryptosystem for identity authentication," *Inf.*, vol. 12, no. 3, pp. 1–14, 2021, doi: 10.3390/info12030104.

[7] S. Praptodiyono, F. Muhammad, and D. Wiriyadinata, "Analysis security system performance MIPv6 in signaling process using AES and Twofish algorithms," *Tek. J. Sains dan Teknol.*, vol. 17, no. 2, p. 158, 2021, doi: 10.36055/tjst.v17i2.13069.

[8] M. R. Alfani, M. Furqan, and Y. R. Nasution, "Pengamanan Data Teks Menggunakan Metode Digital Signature Algorithm (Dsa) Dan Advanced Encryption Standard (Aes)," *J. Sci. Soc. Res.*, vol. 7, no. 1, pp. 301–306, 2024, [Online]. Available: http://jurnal.goretanpena.com/index.php/JSSR

[9] C. Shaik, "Preventing Counterfeit Products using Cryptography, QR Code and Webservice," *Comput. Sci. Eng. An Int. J.*, vol. 11, no. 1, pp. 1–11, 2021, doi: 10.5121/cseij.2021.11101.

[10] S. Ahmad and S. Mehfuz, "Efficient time-oriented latency-based secure data encryption for cloud storage," *Cyber Secur. Appl.*, vol. 2, p. 100027, 2024, doi: 10.1016/j.csa.2023.100027.

[11] A. Yulius, A. Putra, T. Willay, and A. Risky, "Perancangan Aplikasi Pengamanan Data Berbasis Web Dengan Penerapan Algoritma Kriptografi 3Des Dan Twofish," *J. InTekSis*, vol. 10, no. 2, p. 53, 2022.

[12] F. Ahmed *et al.*, "Toward fine-grained access control and privacy protection for video sharing in media convergence environment," *Int. J. Intell. Syst.*, vol. 37, no. 5, pp. 3025–3049, 2022, doi: 10.1002/int.22810.

[13] G. Gafrun and Y. Supit, "Algoritma Tanda Tangan Digital Untuk Meningkatkan Keamanan Pesan," *Simtek J. Sist. Inf. dan Tek. Komput.*, vol. 9, no. 2, pp. 198–204, 2024, doi: 10.51876/simtek.v9i2.1294.

[14] A. Eritza, M. Ramadhan, and H. Hafizah, "Penerapan Digital Signature Metode SHA dan DSA Pada Slip Gaji Pegawai," *J. Sist. Inf. Triguna Dharma (JURSI TGD)*, vol. 1, no. 6, p. 906, 2022, doi: 10.53513/jursi.v1i6.6002.

[15] T. U. Haq, T. Shah, G. F. Siddiqui, M. Z. Iqbal, I. A. Hameed, and H. Jamil, "Improved Twofish Algorithm: A Digital Image Enciphering Application," *IEEE Access*, vol. 9, pp. 76518–76530, 2021, doi: 10.1109/ACCESS.2021.3081792.

[16] F. Fakhrizal, A. B. Pasaribu, S. Wulandari, and R. A. Putri, "Implementasi Security System Menggunakan Kriptografi Algoritma Simetris Untuk Pengamanan Video," *Bigint J. Comput.*, vol. 1, no. 1, pp. 9–18, 2023, [Online]. Available: https://scholar.google.com/citations?view_op=view_citation&hl=en&user=FP0rNUcAAAAJ&pagesize=100&citation_for_view=FP0rNUcAAAAJ:TQgYirikUcIC

This Journal is licensed under a Creative Commons Attribution 4.0 International License.