Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9667

Analisis Perbandingan BLAKE2S dan SHA3-512 dalam Pengujian Ketahanan terhadap Serangan Bruteforce

Rizky Akbar Mokolanot*, Eliasta Ketaren, Mans Lumiu Mananohas
Sistem Informasi, Fakultas Matematika dan Ilmu Pengetahuan Alam, Universitas Sam Ratulangi, Manado, Indonesia
Email: [1,*]rizkymokolanot24@gmail.com, [2]eliasketaren@unsrat.ac.id, [3]mansmananohas@unsrat.ac.id
Email Penulis Korespondensi: rizkymokolanot24@gmail.com*
Submitted: **11/03/2026**; Accepted: **27/03/2026**; Published: **31/03/2026**

Abstrak–Perkembangan teknologi komputasi modern, seperti high-performance computing, cloud computing, dan GPU, telah meningkatkan kemampuan penyerang dalam melakukan serangan *brute force* terhadap sistem kriptografi. Penelitian ini bertujuan untuk menganalisis dan membandingkan ketahanan dua algoritma hash modern, yaitu BLAKE2s dan SHA3-512, terhadap serangan *brute force* dalam konteks pengamanan data berbasis steganografi video. Metode penelitian dilakukan melalui pengujian empiris dengan mengukur waktu cracking, hash rate, serta jumlah percobaan yang dibutuhkan untuk menemukan nilai hash. Hasil penelitian menunjukkan bahwa SHA3-512 memiliki ketahanan yang lebih tinggi dibandingkan BLAKE2s, dengan waktu cracking sebesar 511.479 detik, sementara BLAKE2s hanya membutuhkan 216.156 detik. Perbedaan ini dipengaruhi oleh hash rate BLAKE2s yang lebih tinggi, yaitu 1.350.846 H/s, dibandingkan SHA3-512 sebesar 570.881 H/s, sehingga mempercepat proses *brute force*. Meskipun demikian, waktu embedding kedua algoritma relatif sama, dengan selisih yang tidak signifikan. Jumlah percobaan *brute force* pada kedua algoritma juga identik, yaitu 291.993.781 percobaan, yang menunjukkan bahwa perbedaan ketahanan lebih dipengaruhi oleh efisiensi komputasi daripada kompleksitas ruang pencarian. Dengan demikian, SHA3-512 direkomendasikan sebagai algoritma hash yang lebih aman untuk melindungi data rahasia terhadap serangan *brute force*, meskipun memiliki performa yang lebih rendah dibandingkan BLAKE2s.

Kata Kunci: Brute force; Kriptografi; BLAKE2s; SHA3-512; Hash; Steganografi Video

Abstract-The advancement of modern computing technologies, including high-performance computing, cloud computing, and GPUs, has significantly enhanced attackers' capabilities to perform *brute force* attacks on cryptographic systems. This study aims to analyze and compare the resistance of two modern hash algorithms, BLAKE2s and SHA3-512, against *brute force* attacks in the context of video steganography-based data protection. The research method employs empirical testing by measuring cracking time, hash rate, and the number of attempts required to retrieve hash values. The results indicate that SHA3-512 demonstrates higher resistance compared to BLAKE2s, requiring 511,479 seconds to be cracked, whereas BLAKE2s requires only 216,156 seconds. This difference is attributed to the higher hash rate of BLAKE2s (1,350,846 H/s) compared to SHA3-512 (570,881 H/s), which accelerates the *brute force* process. However, the embedding time for both algorithms is relatively similar, with only a negligible difference. Additionally, both algorithms require the same number of *brute force* attempts (291,993,781), indicating that the difference in resistance is primarily influenced by computational efficiency rather than search space complexity. Therefore, SHA3-512 is recommended as a more secure hash algorithm for protecting sensitive data against *brute force* attacks, despite its lower computational performance compared to BLAKE2s.

Keywords: *Brute force*; Cryptography, BLAKE2s, SHA3-512, Hash Function, Video Steganography

1. PENDAHULUAN

Perkembangan teknologi komputasi modern telah membawa perubahan signifikan dalam lanskap keamanan sistem informasi. Kemajuan pada bidang *high-performance computing*, *cloud computing*, serta pemanfaatan *graphics processing* unit (GPU) memungkinkan proses komputasi dilakukan secara paralel dalam skala besar dengan kecepatan yang sangat tinggi [1]. Di satu sisi, kemajuan ini memberikan keuntungan dalam efisiensi pemrosesan data, namun di sisi lain juga meningkatkan kapabilitas penyerang dalam melakukan berbagai bentuk serangan kriptografi, khususnya serangan *brute force* [2]. Serangan yang sebelumnya dianggap tidak praktis karena keterbatasan sumber daya kini menjadi semakin realistis untuk dilakukan, terutama terhadap sistem yang tidak memiliki mekanisme pengamanan yang memadai [3].

Dalam konteks keamanan modern, fungsi hash kriptografi memainkan peran yang sangat penting. Tidak hanya digunakan dalam penyimpanan kata sandi, algoritma hash juga menjadi komponen utama dalam berbagai aplikasi kritis seperti *blockchain*, digital *forensics*, *secure logging*, *message authentication code* (MAC), serta tanda tangan digital [4]. Fungsi hash diharapkan memiliki sifat satu arah (*one-way function*), tahan terhadap collision, serta memiliki ruang pencarian yang sangat besar sehingga sulit untuk dibalikkan melalui serangan *brute force* [5]. Oleh karena itu, ketahanan algoritma hash terhadap serangan *brute force* menjadi salah satu indikator utama dalam menilai tingkat keamanan suatu sistem informasi.

Perkembangan teknologi juga memunculkan dilema baru dalam desain algoritma hash, yaitu antara efisiensi dan keamanan [6]. Algoritma yang dirancang dengan fokus pada kecepatan komputasi seringkali memberikan performa yang tinggi dalam pemrosesan data, tetapi pada saat yang sama dapat mempercepat proses eksploitasi oleh penyerang melalui serangan *brute force*. Hal ini terutama menjadi perhatian dalam implementasi sistem autentikasi yang tidak dilengkapi dengan mekanisme penguatan tambahan seperti salt, key stretching, atau

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9667

adaptive hashing. Dengan kata lain, semakin cepat suatu algoritma menghasilkan hash, semakin besar pula potensi risiko jika algoritma tersebut digunakan tanpa strategi pengamanan yang tepat.

Salah satu algoritma hash modern yang banyak digunakan adalah BLAKE2s. Algoritma ini merupakan pengembangan dari BLAKE, yang merupakan finalis dalam kompetisi SHA-3 yang diselenggarakan oleh National Institute of Standards and Technology (NIST) [7]. BLAKE2s dirancang untuk memberikan performa tinggi pada platform 32-bit dengan konsumsi sumber daya yang rendah, sehingga sangat cocok digunakan pada perangkat dengan keterbatasan sumber daya (resource-constrained devices) serta aplikasi real-time. Keunggulan utama BLAKE2s terletak pada efisiensi dan kecepatan komputasinya, yang menjadikannya populer dalam berbagai implementasi seperti password hashing, verifikasi integritas file, dan sistem keamanan jaringan. BLAKE2s juga mendukung fitur-fitur tambahan seperti keyed hashing, salt, dan personalization yang memungkinkan fleksibilitas dalam berbagai skenario keamanan tanpa memerlukan konstruksi tambahan seperti HMAC [8]. Hal ini menjadikan BLAKE2s tidak hanya cepat, tetapi juga praktis dalam implementasi sistem keamanan modern. Namun demikian, tingginya kecepatan komputasi yang dimiliki BLAKE2s dapat menjadi pedang bermata dua, karena dalam konteks serangan *brute force*, algoritma yang lebih cepat justru berpotensi mempercepat proses eksploitasi jika tidak diimbangi dengan mekanisme pengamanan tambahan seperti key stretching atau penggunaan parameter adaptif. Oleh karena itu, meskipun BLAKE2s unggul dari sisi performa, evaluasi terhadap ketahanannya terhadap serangan *brute force* tetap menjadi hal yang krusial dalam menentukan tingkat keamanannya dalam implementasi nyata [9].

SHA3-512 merupakan bagian dari standar SHA-3 yang dikembangkan melalui kompetisi global oleh NIST dengan pendekatan konstruksi sponge [10]. Desain ini memberikan tingkat keamanan struktural yang tinggi dan ketahanan yang lebih kuat terhadap berbagai serangan kriptografi, termasuk collision attack, preimage attack, dan *brute force*. Meskipun memiliki performa yang relatif lebih lambat dibandingkan algoritma seperti BLAKE2s, SHA3-512 dikenal memiliki stabilitas dan tingkat keamanan yang tinggi, sehingga sering direkomendasikan untuk aplikasi yang membutuhkan perlindungan data dengan tingkat keamanan maksimal [11]. Konstruksi sponge yang digunakan dalam SHA3-512 memungkinkan fleksibilitas dalam pengolahan input dengan panjang variabel serta memberikan perlindungan yang lebih baik terhadap serangan struktural yang tidak dapat ditangani secara optimal oleh konstruksi Merkle–Damgård pada generasi hash sebelumnya [12]. Selain itu, SHA3-512 memiliki kapasitas internal (capacity) yang besar, sehingga meningkatkan kompleksitas serangan dan memperluas ruang pencarian secara signifikan. Hal ini membuat algoritma ini lebih tahan terhadap eksploitasi berbasis komputasi masif, termasuk serangan yang memanfaatkan paralelisme GPU dan komputasi terdistribusi [13].

Sejumlah penelitian terdahulu menunjukkan bahwa tidak terdapat algoritma hash yang unggul secara mutlak dalam semua aspek [14][15][16]. Beberapa studi mengindikasikan bahwa SHA-3 memiliki keunggulan dalam konsistensi avalanche effect dan keamanan struktural, sementara BLAKE2 unggul dalam efisiensi waktu pemrosesan. Dalam konteks sistem terdistribusi seperti blockchain, pemilihan algoritma hash seringkali disesuaikan dengan kebutuhan spesifik sistem, termasuk tingkat ancaman, kapasitas komputasi, serta efisiensi energi. Hal ini menunjukkan bahwa pemilihan algoritma hash tidak dapat dilakukan secara umum, melainkan harus mempertimbangkan skenario penggunaan yang spesifik. dinamika perkembangan teknologi komputasi modern turut memengaruhi relevansi hasil-hasil penelitian sebelumnya, sehingga evaluasi terhadap algoritma hash perlu dilakukan secara berkelanjutan dengan mempertimbangkan konteks implementasi terkini. Faktor seperti kemampuan paralelisme GPU, optimasi perangkat keras, serta pola serangan yang semakin adaptif menjadikan analisis komparatif tidak hanya penting secara teoretis, tetapi juga secara praktis. Oleh karena itu, diperlukan pendekatan evaluasi yang tidak hanya menitikberatkan pada performa atau keamanan secara terpisah, melainkan mampu mengintegrasikan kedua aspek tersebut dalam satu kerangka analisis yang komprehensif dan kontekstual [17].

Sebagian besar penelitian sebelumnya masih berfokus pada pengujian performa algoritma hash atau analisis teoretis terhadap tingkat keamanannya. Kajian empiris yang secara langsung membandingkan ketahanan algoritma hash terhadap serangan *brute force* dalam skenario implementasi nyata masih relatif terbatas. Padahal, pendekatan empiris sangat penting untuk memahami bagaimana karakteristik algoritma, khususnya efisiensi komputasi, memengaruhi kecepatan dan efektivitas serangan *brute force* ketika dihadapkan pada kemampuan komputasi modern.

Penelitian ini dilakukan untuk menganalisis dan membandingkan ketahanan dua algoritma hash modern, yaitu BLAKE2s dan SHA3-512, terhadap serangan *brute force*. Penelitian ini tidak hanya berfokus pada aspek teoretis, tetapi juga mengedepankan pengujian empiris dengan mengukur waktu cracking, hash rate, serta jumlah percobaan yang diperlukan dalam proses *brute force*. Selain itu, penelitian ini juga mengkaji implikasi penggunaan kedua algoritma dalam konteks pengamanan data berbasis steganografi video, yang merupakan salah satu teknik penyembunyian informasi yang banyak digunakan dalam sistem keamanan digital.

Hasil penelitian ini diharapkan dapat memberikan kontribusi dalam bentuk landasan empiris yang lebih kuat bagi pengembang sistem dan praktisi keamanan informasi dalam memilih algoritma hash yang tepat. Dengan memahami trade-off antara efisiensi dan keamanan, diharapkan implementasi sistem kriptografi di masa depan dapat lebih adaptif terhadap perkembangan teknologi sekaligus tetap mampu menghadapi ancaman serangan *brute force* yang semakin kompleks.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9667

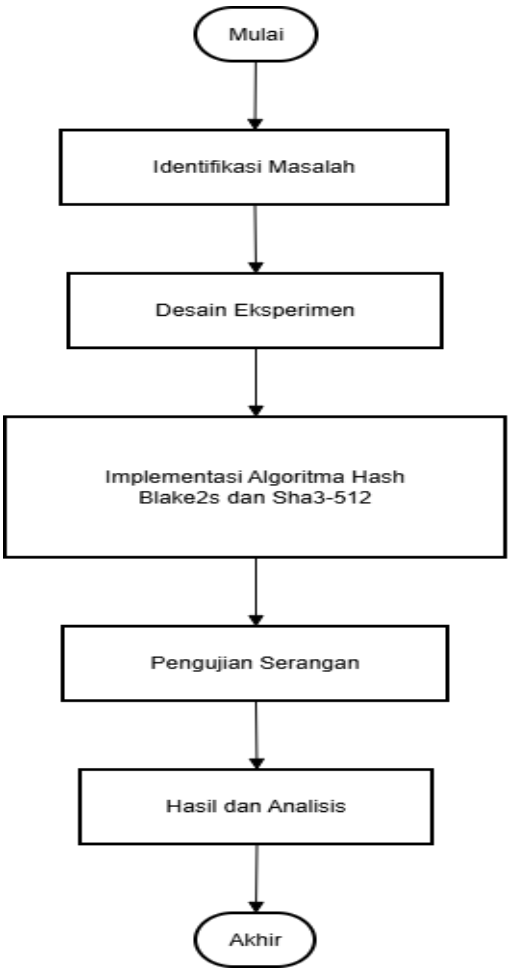
2. METODOLOGI PENELITIAN

2.1 Jenis dan Pendekatan Penelitian

Penelitian ini menggunakan metode eksperimental dengan menerapkan algoritma hash BLAKE2s dan SHA3-512 sebagai objek utama dalam pengujian ketahanan terhadap serangan *brute force*. Objek penelitian yang digunakan berupa data digital yang disembunyikan dalam media video melalui teknik steganografi, kemudian diamankan menggunakan kedua algoritma hash tersebut. Proses penelitian dilakukan dengan menghasilkan nilai hash dari data yang telah disisipkan, selanjutnya dilakukan simulasi serangan *brute force* untuk mengukur tingkat ketahanan masing-masing algoritma. Pengujian difokuskan pada beberapa parameter utama, yaitu waktu yang dibutuhkan untuk proses cracking, hash rate, serta jumlah percobaan yang diperlukan untuk menemukan nilai hash yang sesuai [18]. Melalui pendekatan ini, penelitian bertujuan untuk memperoleh perbandingan empiris mengenai efektivitas dan ketahanan BLAKE2s dan SHA3-512 dalam menghadapi ancaman serangan *brute force* pada kondisi komputasi modern.

2.2 Tahapan Penelitian

Rangkaian tahapan penelitian yang digunakan pada penelitian ini dapat dilihat pada Gambar 1.



Gambar 1. Tahapan Penelitian

Rangkaian tahapan penelitian ini disusun secara sistematis untuk memastikan proses analisis berjalan terstruktur dan menghasilkan temuan yang valid. Penelitian diawali dengan tahap penentuan topik dan ruang lingkup kajian yang berfokus pada keamanan algoritma hash terhadap serangan *brute force*. Selanjutnya dilakukan identifikasi masalah dengan mengkaji berbagai kerentanan keamanan data, khususnya yang berkaitan dengan meningkatnya ancaman serangan *brute force* seiring perkembangan teknologi komputasi modern [19].

Tahap berikutnya adalah desain eksperimen, di mana peneliti menetapkan algoritma yang akan diuji, yaitu BLAKE2s dan SHA3-512, serta menentukan parameter pengujian seperti panjang password, tingkat kompleksitas, dan skenario serangan *brute force* yang digunakan. Setelah itu, dilakukan implementasi algoritma hash menggunakan bahasa pemrograman Python dengan memanfaatkan library kriptografi yang relevan.

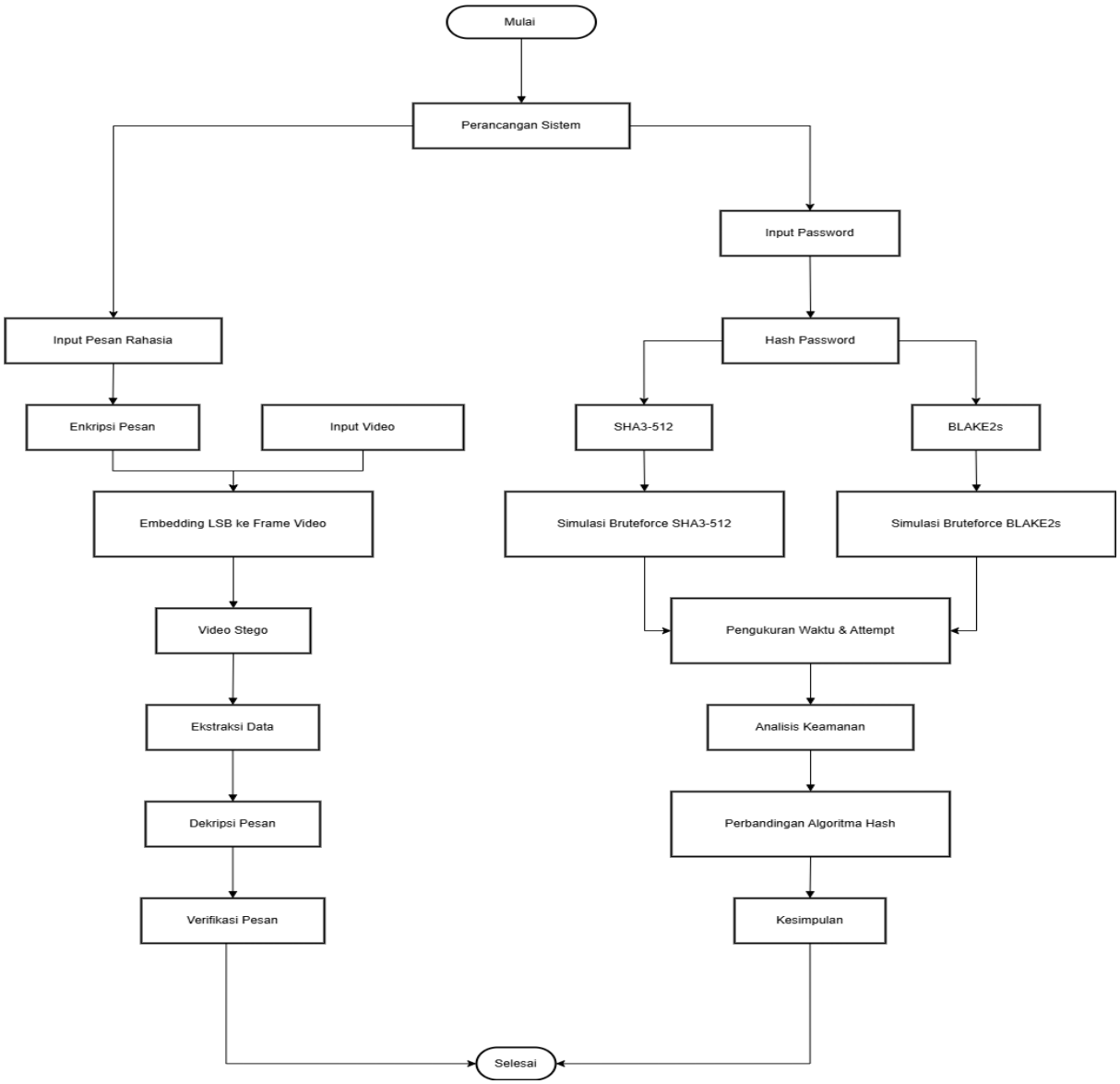
Proses penelitian kemudian dilanjutkan dengan pengujian serangan *brute force* terhadap kedua algoritma. Pada tahap ini dilakukan simulasi untuk mengukur kinerja masing-masing algoritma dengan mencatat waktu yang dibutuhkan untuk cracking, jumlah percobaan yang dilakukan, serta hash rate yang dihasilkan. Data yang

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9667

diperoleh selanjutnya dianalisis untuk membandingkan performa dan tingkat ketahanan BLAKE2s dan SHA3-512 terhadap serangan *brute force*. Tahap akhir penelitian adalah penarikan kesimpulan sebagai hasil dari keseluruhan proses yang telah dilakukan [20].

2.3 Flowchart Sistem

Adapun gambaran alur sistem seperti pada gambar 2.



Gambar 2. Diagram Alur Penelitian

Gambar 2 menggambarkan alur sistem secara menyeluruh yang diawali dari tahap mulai dan perancangan sistem, kemudian terbagi menjadi dua jalur utama, yaitu proses steganografi dan proses pengujian keamanan hash. Jalur kiri menampilkan proses steganografi yang dimulai dari input pesan rahasia dan input video, dilanjutkan dengan enkripsi pesan sebelum dilakukan proses embedding LSB ke dalam frame video hingga menghasilkan video stego. Setelah video stego terbentuk, sistem melakukan ekstraksi data, dekripsi pesan, dan verifikasi pesan untuk memastikan bahwa pesan yang disisipkan dapat dikembalikan dengan benar.

Sementara itu, jalur kanan menampilkan proses evaluasi keamanan yang dimulai dari input password yang kemudian diproses melalui hash password. Password tersebut di-hash menggunakan dua algoritma secara paralel, yaitu SHA3-512 dan BLAKE2s. Hasil hash dari masing-masing algoritma kemudian diuji melalui simulasi *brute force*, dilanjutkan dengan pengukuran waktu dan jumlah attempt. Tahap berikutnya adalah analisis keamanan dan perbandingan algoritma hash untuk mengetahui performa serta tingkat ketahanannya, hingga akhirnya menghasilkan kesimpulan penelitian. Kedua jalur tersebut bermuara pada tahap selesai sebagai akhir dari keseluruhan proses sistem.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9667

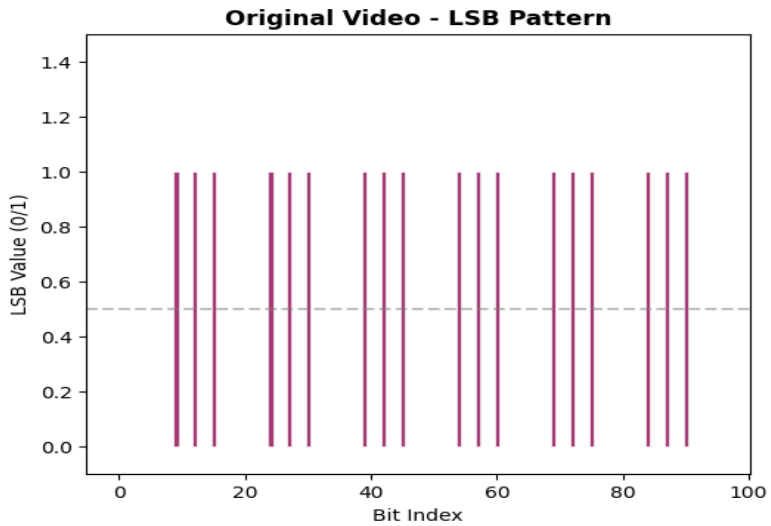
3. HASIL DAN PEMBAHASAN

3.1 Hasil Penelitian

Penelitian ini menganalisis ketahanan dua algoritma hash kriptografi, yaitu SHA3-512 dan BLAKE2s, terhadap serangan *brute force* dalam konteks steganografi video. Pengujian dilaksanakan menggunakan file video berdurasi 55 detik dengan resolusi 1920x1080 pixel (1080p) dan ukuran 2,96 MB sebagai media penampung. Data rahasia berupa file teks sepanjang 223 karakter disisipkan ke dalam video melalui teknik LSB (Least Significant Bit) steganography, kemudian dilindungi dengan hash password menggunakan kedua algoritma tersebut. Serangan *brute force* dilakukan dengan charset gabungan huruf kecil dan angka (a-z, 0-9) sebanyak 36 karakter, terhadap password sepanjang 6 karakter yang menghasilkan total 2,176,782,336 kombinasi kemungkinan.

3.1.1 Proses Embedding Data

Proses embedding dilakukan dengan memodifikasi bit terkecil (LSB) pada setiap pixel di frame video. Pada penelitian ini, data rahasia dikonversi menjadi representasi biner dan disisipkan pada saluran warna Red channel dari frame pertama video. Teknik ini memastikan perubahan pada nilai pixel hanya sebesar ±1, sehingga secara visual tidak dapat dideteksi oleh mata manusia. Dari analisis LSB embedding yang dilakukan SHA3-512 mengubah 95 bit (49.48%) dari 192 bit yang dianalisis dan BLAKE2s mengubah 84 bit (43.75%) dari 192 bit yang dianalisis.

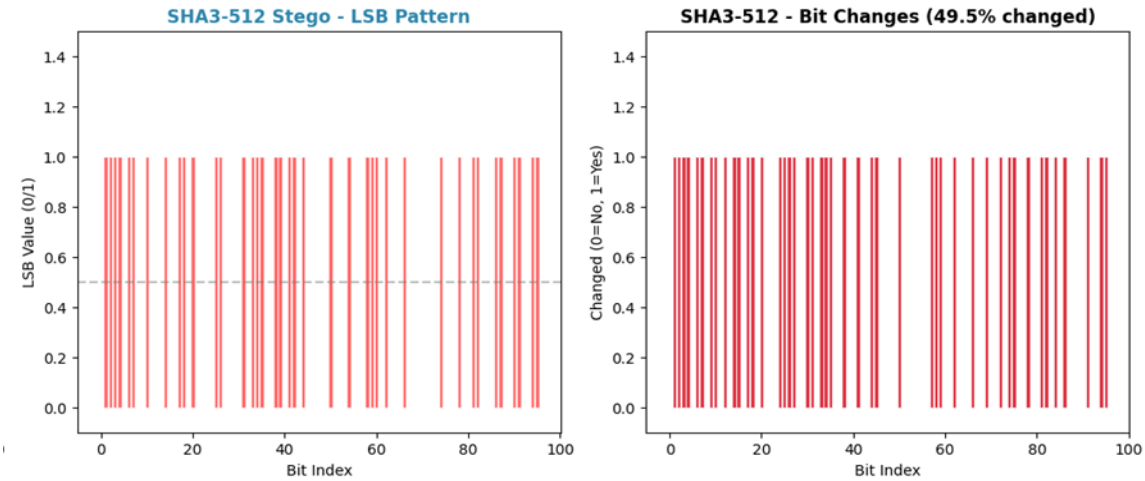


Gambar 3. Original Video LSB Pattern SHA3-512 dan BLAKE2S

Garis-garis vertikal yang muncul menunjukkan posisi bit yang bernilai 0 atau 1 pada beberapa titik tertentu, sementara garis putus-putus di tengah menggambarkan batas rata-rata distribusi antara kedua nilai tersebut. Secara umum, pola yang terlihat cenderung tersebar dan tidak membentuk struktur tertentu, menunjukkan bahwa distribusi bit pada video asli masih bersifat alami dan acak. Hal ini penting dalam konteks steganografi LSB karena penyisipan pesan nantinya akan mengubah sebagian nilai bit paling rendah tersebut. Jika metode embedding dilakukan dengan baik, perubahan setelah penyisipan tetap akan mempertahankan pola distribusi yang tampak acak seperti pada gambar ini, sehingga keberadaan pesan tersembunyi sulit dideteksi baik secara visual maupun melalui analisis statistik sederhana.

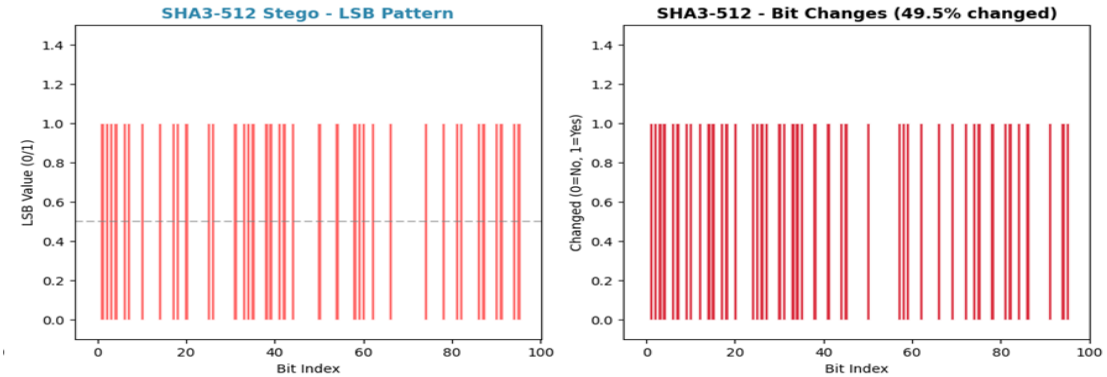
Perubahan bit yang terjadi setelah proses hashing menggunakan algoritma SHA3-512 dan BLAKE2s pada gambar 4, Grafik menunjukkan posisi bit (Bit Index) pada sumbu horizontal dan status perubahan bit pada sumbu vertikal, di mana nilai 0 menunjukkan tidak terjadi perubahan, sedangkan 1 menunjukkan bit mengalami perubahan dibandingkan dengan data awal.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9667



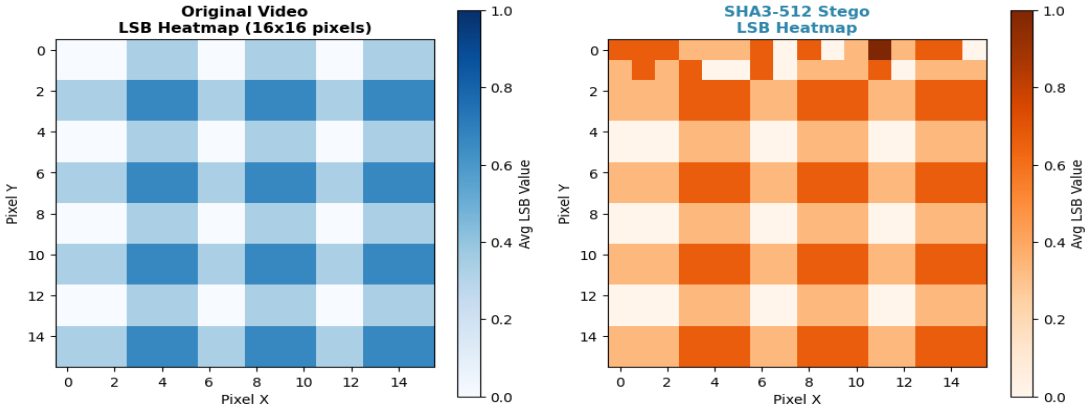
Gambar 4. Bit Changes SHA3-512 dan BLAKE2S

Pada grafik SHA3-512 terlihat bahwa sekitar 49,5% bit mengalami perubahan, yang ditunjukkan oleh banyaknya garis vertikal pada nilai 1. Hal ini menunjukkan bahwa hampir setengah dari total bit output berubah ketika terjadi modifikasi kecil pada input. Persentase ini mendekati 50%, yang merupakan karakteristik ideal dari suatu fungsi hash kriptografis dalam menghasilkan efek avalanche (Avalanche Effect).Sementara itu pada grafik BLAKE2s terlihat bahwa sekitar 43,8% bit mengalami perubahan. Meskipun sedikit lebih rendah dibandingkan SHA3-512, nilai ini tetap menunjukkan distribusi perubahan yang cukup merata di berbagai posisi bit. Perubahan yang tersebar secara acak dan tidak terpusat pada indeks tertentu menunjukkan bahwa algoritma bekerja dengan baik dalam menyebarkan perubahan input ke seluruh output hash.Secara keseluruhan, kedua algoritma menunjukkan sifat difusi yang baik, namun SHA3-512 memiliki tingkat perubahan bit yang sedikit lebih mendekati kondisi ideal 50%, sehingga secara teoritis menunjukkan efek avalanche yang lebih kuat dibandingkan BLAKE2s pada pengujian ini.



Gambar 5. Original and Byte Change Stego SHA3-512

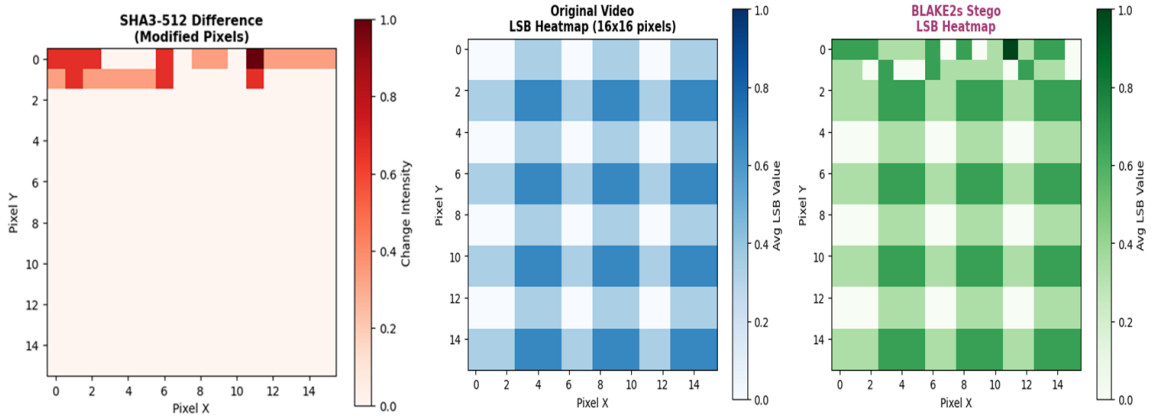
Visualisasi heatmap LSB (Least Significant Bit) dalam tiga bagian pada gambar 5, yaitu LSB video asli, LSB hasil steganografi menggunakan SHA3-512, dan perbedaan piksel yang dimodifikasi.Pada heatmap pertama (Original Video LSB Heatmap), terlihat pola distribusi LSB yang masih terstruktur mengikuti pola piksel asli.



Gambar 6. LSB Heatmap SHA3-512

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9667

Warna yang ditampilkan menunjukkan nilai rata-rata LSB pada blok piksel berukuran 16×16. Pada heatmap kedua (SHA3-512 Stego LSB Heatmap), distribusi warna tampak lebih menyebar dan mengalami perubahan dibandingkan pola awal. Hal ini menunjukkan bahwa proses penyisipan data menggunakan SHA3-512 memodifikasi nilai LSB pada sejumlah piksel. Heatmap ketiga (SHA3-512 Difference) memperlihatkan lokasi piksel yang mengalami perubahan. Area berwarna merah menunjukkan piksel yang dimodifikasi, sedangkan area terang menunjukkan tidak ada perubahan. Terlihat bahwa perubahan hanya terjadi pada sebagian kecil area dan tersebar secara tidak beraturan. Hal ini menunjukkan bahwa penyisipan data bersifat terdistribusi dan tidak terkonsentrasi pada satu wilayah tertentu, sehingga membantu menjaga kualitas visual video tetap stabil.



Gambar 6. SHA3-512 Difference (Modified Pixels) dan LSB Heatmap BLAKE2S

Pada heatmap BLAKE2s Stego LSB, terlihat adanya perubahan distribusi nilai LSB dibandingkan dengan kondisi asli. Pola warna menunjukkan bahwa penyisipan data mempengaruhi sejumlah blok piksel, meskipun tidak mengubah struktur keseluruhan secara drastis.Pada heatmap Difference BLAKE2s, area berwarna merah menunjukkan piksel yang dimodifikasi. Perubahan tampak tersebar pada beberapa bagian tertentu, dengan jumlah yang relatif terbatas. Dibandingkan dengan SHA3-512, pola perubahan terlihat sedikit lebih terkonsentrasi pada area tertentu, meskipun tetap tidak membentuk pola yang mudah dikenali.

Total bit yang dianalisis pada kedua metode adalah 192 bit. SHA3-512 mengubah 95 bit (49,48%), sedangkan BLAKE2s mengubah 84 bit (43,75%). Nilai rata-rata frame asli sebesar 4,01 meningkat menjadi 4,24 pada SHA3-512 dan 4,20 pada BLAKE2s setelah embedding. Selisih nilai pada SHA3-512 sebesar 0,2344, sementara pada BLAKE2s sebesar 0,1979. Data ini menunjukkan bahwa secara kuantitatif BLAKE2s menghasilkan perubahan rata-rata yang lebih kecil dibandingkan SHA3-512, sehingga dapat dikatakan lebih stabil dalam mempertahankan karakteristik statistik frame asli setelah proses penyisipan pesan.

Tabel 1. LSB Embedding Statistics Summary

Metrik	SHA3-512	BLAKE2s
Total Bit yang Dianalisis	192	192
Jumlah Bit Berubah	95	84
Persentase Perubahan	49,48%	43,75%
Nilai Rata-rata Asli	4,01	4,01
Nilai Rata-rata Stego	4,24	4,20

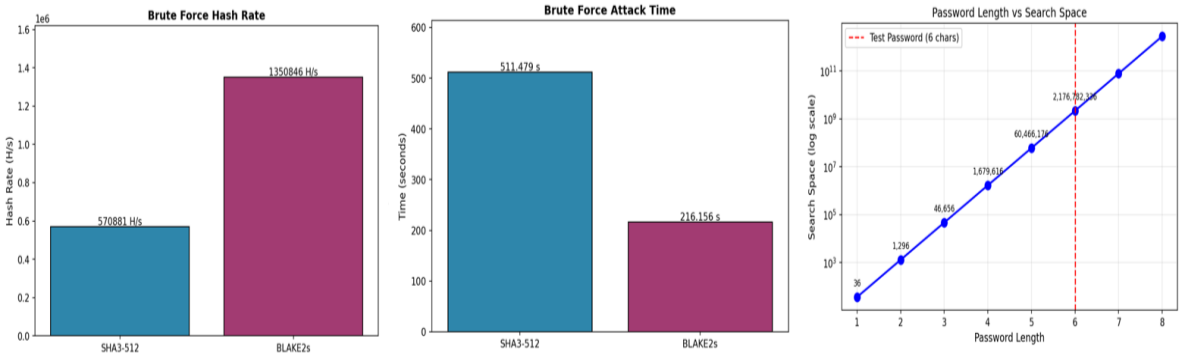
Tabel 1 menunjukkan bahwa total bit yang dianalisis pada kedua metode adalah 192 bit. SHA3-512 mengubah 95 bit (49,48%), sedangkan BLAKE2s mengubah 84 bit (43,75%). Nilai rata-rata frame asli sebesar 4,01 meningkat menjadi 4,24 pada SHA3-512 dan 4,20 pada BLAKE2s setelah embedding. Selisih nilai pada SHA3-512 sebesar 0,2344, sementara pada BLAKE2s sebesar 0,1979. Data ini menunjukkan bahwa secara kuantitatif BLAKE2s menghasilkan perubahan rata-rata yang lebih kecil dibandingkan SHA3-512, sehingga dapat dikatakan lebih stabil dalam mempertahankan karakteristik statistik frame asli setelah proses penyisipan pesan.

3.1.2 Hasil Serangan *Brute force*

Serangan *brute force* dilaksanakan dengan mengekstrak hash digest dari video yang telah di-embed, kemudian mencoba seluruh kombinasi password secara sistematis hingga hash yang cocok ditemukan. Pengujian menggunakan 16 core CPU secara paralel melalui multiprocessing untuk memaksimalkan throughput komputasi. Kedua algoritma berhasil ditemukan passwordnya, yaitu "d23wde", setelah melewati 291,993,781 percobaan. SHA3-512 memerlukan waktu 511.479 detik untuk menyelesaikan serangan *brute force* dengan hash rate sebesar 570,881 hash per detik. Sebaliknya, BLAKE2s berhasil di-crack dalam waktu 216.156 detik dengan hash

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9667

rate sebesar 1,350,846 hash per detik. Perbedaan waktu serangan antara kedua algoritma mencapai 295.32 detik, di mana SHA3-512 membutuhkan waktu lebih lama hingga 136.6% dibandingkan BLAKE2s. Jumlah total percobaan pada kedua algoritma identik karena *brute force* menggunakan charset dan panjang password yang sama, sehingga perbedaan waktu sepenuhnya disebabkan oleh perbedaan kecepatan komputasi hash.



Gambar 7. Bruteforce Attack time, Bruteforce Hash Rate, dan Bruteforce Complexity Analysis

3.1.3 Perincian Waktu Total

Waktu total mencakup seluruh siklus dari proses embedding hingga serangan *brute force* berhasil menemukan password. Untuk SHA3-512, total waktu yang diperlukan adalah 511.72 detik, dengan dominasi pada fase *brute force* sebesar 511.48 detik (99.95% dari total waktu). Untuk BLAKE2s, total waktu adalah 216.38 detik, dengan fase *brute force* memakan waktu 216.16 detik (99.90% dari total waktu). Hal ini menunjukkan bahwa proses embedding hanya mengambil porsi yang sangat kecil dari seluruh durasi, dan keamanan algoritma sangat ditentukan oleh ketahanan hash terhadap serangan *brute force*.

Tabel 2. Perincian Waktu Total, Percobaan , Embedding dan *Brute force*

Metrik	*SHA3-512*	*BLAKE2s*	Selisih
Waktu Embedding	0,2373 detik	0,226 detik	0,0111s
Waktu *Brute force*	511,48 detik	216,16 detik	295,32 detik
Total Waktu	511,72 detik	216,38	295,33 detik
Total Percobaan	291,993,781	291,993,781	-
Embedding	0.05%	0,10%	-
BruteForce	99,95%	99,90%	-

Tabel 2 di atas menyajikan rekapitulasi hasil seluruh metrik pengujian Dari hasil tersebut terlihat bahwa BLAKE2s sedikit unggul dalam efisiensi embedding, namun SHA3-512 jauh lebih unggul dalam hal ketahanan terhadap serangan *brute force*. Skor keamanan SHA3-512 mencapai 100,0 dari 100 (berdasarkan rasio waktu *brute force* terhadap nilai maksimum), sedangkan BLAKE2s hanya mendapatkan skor 42.3 dari 100. skor 56,3 dari 100.

3.2 Pembahasan

3.2.1 Ketahanan Terhadap Serangan *Brute force*

Hasil pengujian secara jelas menunjukkan bahwa SHA3-512 memiliki ketahanan yang lebih tinggi terhadap serangan *brute force* dibandingkan BLAKE2s. SHA3-512 membutuhkan waktu 511.479 detik untuk di-crack, sedangkan BLAKE2s hanya memerlukan 216.156 detik. Perbedaan yang signifikan ini dapat dijelaskan melalui dua faktorutama.Pertama, panjang digest SHA3-512 mencapai 512 bit, jauh lebih besar dibandingkan BLAKE2s yang hanya menghasilkan digest sepanjang 256 bit. Meskipun dalam pengujian ini *brute force* ditargetkan pada password bukan langsung pada hash output, perbedaan panjang digest mempengaruhi kecepatan komputasi hash secara keseluruhan. Algoritma dengan output yang lebih panjang dan struktur komputasi yang lebih kompleks (sponge construction pada SHA3-512) membutuhkan lebih banyak sumber daya komputasi per operasi hash. Kedua, hash rate SHA3-512 tercatat sebesar 570,881 H/s, sedangkan BLAKE2s mencapai 1,350,846 H/s. Hash rate BLAKE2s lebih tinggi hingga 136.6% dibandingkan SHA3-512. Hal ini mencerminkan desain BLAKE2s yang memang dioptimalkan untuk kecepatan dan efisiensi komputasi. Namun, kecepatan tinggi ini justru menjadi kerentanan dari perspektif keamanan, karena penyerang dapat menjalankan lebih banyak percobaan *brute force* dalam satuan waktu yang sama.

3.2.2 Efisiensi Proses Embedding

Dari segi efisiensi embedding, kedua algoritma menunjukkan performa yang hampir setara. SHA3-512 membutuhkan 0.237 detik dan BLAKE2s membutuhkan 0.226 detik, dengan selisih hanya 0.011 detik.

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9667

Persamaan ini wajar karena proses embedding pada dasarnya adalah operasi manipulasi bit pada pixel video, yang tidak bergantung secara signifikan pada algoritma hash yang digunakan. Hash password hanya dihitung sekali di awal proses sebelum embedding dimulai, sehingga perbedaan kecepatan hashing tidak memberikan dampak berarti pada durasi embedding secara keseluruhan.

3.2.3 Analisis Trade-off Keamanan dan Efisiensi

Penelitian ini mengkonfirmasi adanya trade-off yang signifikan antara efisiensi komputasi dan ketahanan keamanan pada algoritma hash. BLAKE2s menawarkan kecepatan hashing yang lebih tinggi dan efisiensi komputasi yang lebih baik, menjadikannya pilihan ideal untuk aplikasi yang membutuhkan throughput tinggi namun tidak menghadapi ancaman *brute force* yang berat, seperti integritas data pada sistem file atau checksumming. Di sisi lain, SHA3-512 memberikan perlindungan yang lebih kuat terhadap serangan *brute force* akibat struktur sponge construction yang lebih kompleks dan output digest yang lebih panjang. Temuan ini sejalan dengan hasil penelitian sebelumnya oleh [21] yang menyatakan bahwa SHA-3 lebih konsisten dalam menjaga integritas data, sedangkan BLAKE2 lebih unggul dalam efisiensi waktu. Demikian pula, [22] menemukan bahwa BLAKE2b 58,64% lebih cepat dibandingkan SHA-256 dalam implementasi blockchain, yang menunjukkan pola yang konsisten bahwa keluarga BLAKE selalu memprioritaskan kecepatan.

4. KESIMPULAN

SHA3-512 memiliki ketahanan yang lebih tinggi terhadap serangan *brute force* dibandingkan BLAKE2s. SHA3-512 membutuhkan waktu 511.479 detik untuk di-crack, sedangkan BLAKE2s hanya memerlukan 216.156 detik. Hal ini menunjukkan bahwa SHA3-512 lebih aman dalam melindungi data yang disembunyikan melalui steganografi video dari upaya serangan *brute force*. BLAKE2s memiliki hash rate yang lebih tinggi sebesar 1,350,846 H/s dibandingkan SHA3-512 yang hanya mencapai 570,881 H/s. Tingginya hash rate BLAKE2s menyebabkan serangan *brute force* dapat dijalankan lebih cepat, sehingga ketahanan keamanannya terhadap serangan tersebut lebih rendah dibandingkan SHA3-512. Waktu embedding kedua algoritma menunjukkan hasil yang hampir setara, dengan SHA3-512 membutuhkan 0.237 detik dan BLAKE2s membutuhkan 0.226 detik. Perbedaan selisih hanya 0.011 detik ini menunjukkan bahwa efisiensi embedding tidak secara signifikan dipengaruhi oleh pilihan algoritma hash yang digunakan.Jumlah percobaan *brute force* pada kedua algoritma identik, yaitu 291,993,781 percobaan. Perbedaan waktu serangan sepenuhnya disebabkan oleh perbedaan kecepatan komputasi hash antara kedua algoritma, bukan perbedaan kompleksitas ruang pencarian. Hasil ini mengkonfirmasi bahwa SHA3-512 adalah algoritma hash yang lebih direkomendasikan untuk melindungi data rahasia yang disembunyikan dalam video terhadap ancaman serangan *brute force*.

REFERENCES

[1] J. Li, “Distributed data processing and task scheduling based on GPU parallel computing,” *Neural Comput. Appl.*, vol. 37, no. 4, pp. 1757–1769, 2025.
[2] B. Hanindhito, A. Fathi, D. Gourounas, D. Trenev, A. Gerstlauer, and L. K. John, “Technology trends in computing hardware and their impacts on high-performance scientific computing Part II: Memory systems, interconnects, and system integration,” *Int. J. High Perform. Comput. Appl.*, p. 10943420251347460, 2026.
[3] F. Lyu, Y. Kang, and S. Wang, “Converging high-performance computing and machine learning for geospatial discovery and innovation,” *Ann. GIS*, pp. 1–22, 2026.
[4] F. Kurniawan, A. Muzakky, N. A. Mulyono, and A. F. Matondang, “Implementasi Teknik Hibrida Enkripsi Aes Dan Steganografi Multi-Platform Pada Aplikasi Berbasis Web’Steganoid’,” *JIKUM J. Ilmu Komput.*, vol. 2, no. 2, pp. 184–189, 2026.
[5] E. Fathalla and M. Azab, “Beyond classical cryptography: A systematic review of post-quantum hash-based signature schemes, security, and optimizations,” *IEEE access*, vol. 12, pp. 175969–175987, 2024.
[6] A. Sarkar, S. R. Chatterjee, and M. Chakraborty, “Role of cryptography in network security,” in *The" essence" of network security: an end-to-end panorama*, Springer, 2020, pp. 103–143.
[7] S. Shaik, “Optimizing Authenticated Encryption: Enhancements and Performance Analysis of ChaCha20 and Blake3 Algorithms,” in *International Conference on Emerging Trends in Mathematical Sciences & Computing*, 2024, pp. 181–193.
[8] A. Sadeghi-Nasab and V. Rafe, “A comprehensive review of the security flaws of hashing algorithms,” *J. Comput. Virol. Hacking Tech.*, vol. 19, no. 2, pp. 287–302, 2023.
[9] R. Sujeetha, J. Aravida Raaja, P. Preeti Charishma, and H. Surya, “CipherHash: A Comprehensive and Secure Solution for Safeguarding Confidentiality and Protecting Sensitive Documents,” in *International Conference on Innovations and Advances in Cognitive Systems*, 2025, pp. 155–166.
[10] K. Tran-Hoang and H. Nakajo, “Kyress: a secure, scalable, and resource-efficient CRYSTALS-Kyber cryptosystem for low-cost embedded devices,” *J. Supercomput.*, vol. 82, no. 2, p. 101, 2026.
[11] F. Li, X. Zhang, J. Feng, J. Ai, Z. Zilic, and J. Wang, “Efficient Hardware Architecture for the Kyber Public-Key Encryption Primitive,” *IEEE Internet Things J.*, 2026.
[12] R. A. Purba *et al.*, *Rekayasa Perangkat Lunak Berorientasi Objek: Teori dan Implementasi*. Yayasan Kita Menulis, 2024.
[13] S. Suryawanshi, D. Saha, and S. Sachan, “New results on the SymSum distinguisher on round-reduced SHA3,” in

Jurnal Sistem Komputer dan Informatika (JSON)
Volume 7, Nomor 3, Maret 2026
e-ISSN 2685-998X
DOI 10.30865/json.v7i3.9667

International Conference on Cryptology in Africa, 2020, pp. 132–151.

[14] P. Peng and M. M. Moghimi, "Hash-based lightweight recommendation in edge computing for privacy-preserving sport communities," *J. Cloud Comput.*, vol. 15, no. 1, p. 7, 2026.

[15] E. T. Ong *et al.*, "THE 5E INQUIRY LEARNING MODEL: ITS EFFECT ON THE LEARNING OF ELECTRICITY AMONG MALAYSIAN STUDENTS," *J. Cakrawala Pendidik.*, vol. 40, no. 1, 2021.

[16] D. ting Liu, B. yuan Cui, X. jun Dai, Z. qiong Zhang, and Y. ming Liu, "A comprehensive evaluation method for crowd-sourcing design work of product appearance integrating fractal dimension and hash algorithm," *Proc. Inst. Mech. Eng. Part B J. Eng. Manuf.*, p. 09544054261416164, 2024.

[17] N. Mhatre and S. Bhattacharjee, "A Hash-Based Nature-Inspired Algorithm for High-Utility Itemset Mining," in *International Conference on Computing and Machine Learning*, 2025, pp. 107–120.

[18] A. Alshahrani, E. Jaha, and N. Alowidi, "Fusion of hash-based hard and soft biometrics for enhancing face image database search and retrieval," *Comput. Mater. Contin.*, vol. 77, no. 3, p. 3489, 2023.

[19] R. A. Purba, "Application design to help predict market demand using the waterfall method," *Matrix J. Manaj. Teknol. dan Inform.*, vol. 11, no. 3, pp. 140–149, 2021.

[20] R. Verma, N. Dhanda, and V. Nagar, "Enhancing security with in-depth analysis of brute-force attack on secure hashing algorithms," in *Proceedings of Trends in Electronics and Health Informatics: TEHI 2021*, Springer, 2022, pp. 513–522.

[21] P. Thavamani, B. T. H. Prasath, N. M. Rashed, R. V. Raman, E. N. Karthick, and K. Venkatesh, "Parallel brute-force decryption tool with grammar and structure validation for enhanced cryptographic cracking efficiency," in *Information and Communication Systems*, CRC Press, 2026, pp. 25–31.

[22] S. Pocarovsky, L. Kockovic, M. Orgon, and R. Róka, "Computational Efficiency of Brute-Force Attacks on Hashing Algorithms," in *Computer Science On-line Conference*, 2025, pp. 402–413.