Jurnal Ilmiah Matematika dan Pendidikan Matematika (JMP)
Vol. 18 No. 1, Juni 2026, hal. 63-74
ISSN (Cetak) : 2085-1456; ISSN (*Online*) : 2550-0422

PERBANDINGAN ALGORITMA *HASH FUNCTION* MD5, SHA-1 DAN SHA-256 DALAM MENJAGA INTEGRITAS DATA PADA SISTEM FILE GAMBAR

Welly Dona Permatasari

Program Studi Matematika, FMIPA, Universitas Mulawarman, Indonesia
wellydona31@email.com

Qonita Qurrota A'yun*

Program Studi Matematika, FMIPA, Universitas Mulawarman, Indonesia
qonitaqurrota@fmipa.unmul.ac.id

Rafika Husnia Munfa'ati

Program Studi Matematika, FMIPA, Universitas Mulawarman, Indonesia
rafikahm@fmipa.unmul.ac.id

ABSTRACT. *Cryptography plays an important role in maintaining digital data integrity, particularly image files vulnerable to alteration and manipulation. This study compares the MD5, SHA-1, and SHA-256 hash algorithms in detecting changes in 30 JPG-format student identification card (e-KTM) image files. Testing was conducted through single-pixel modification and file compression, with analysis based on hash value changes, hashing time, and avalanche effect. The results show that all algorithms successfully detected file modifications through changes in hash values. For single-pixel modification, the avalanche effect ranged from* $78.13\% - 100\%$ *for MD5,* $82.50\% - 100\%$ *for SHA-1, and* $87.50\% - 100\%$ *for SHA-256. For file compression, the ranges were* $81.25\% - 100\%$*,* $85.00\% - 100\%$*, and* $87.50\% - 98.44\%$*, respectively. These results indicate that SHA-256 provides more consistent sensitivity to data changes than MD5 and SHA-1.*

Keywords*: Hash Function, Image Data Integrity, MD5, SHA-1, SHA-256.*

ABSTRAK. Kriptografi berperan penting dalam menjaga integritas data digital, khususnya file gambar yang rentan mengalami perubahan atau manipulasi. Penelitian ini bertujuan membandingkan algoritma *hash* MD5, SHA-1, dan SHA-256 dalam mendeteksi perubahan pada 30 file gambar e-KTM berformat JPG. Pengujian dilakukan melalui perubahan satu piksel dan kompresi file, kemudian dianalisis berdasarkan perubahan nilai hash, waktu proses hashing, dan efek *avalanche*. Hasil penelitian menunjukkan bahwa ketiga algoritma mampu mendeteksi perubahan data dengan baik melalui perubahan nilai hash setelah file dimodifikasi. Pada perlakuan perubahan satu piksel, nilai efek *avalanche* berada pada rentang $78{,}13\% - 100\%$ untuk MD5, $82{,}50\% - 100\%$ untuk SHA-1, dan $87{,}50\% - 100\%$ untuk SHA-256. Pada perlakuan kompresi file, nilai efek *avalanche* berada pada rentang $81{,}25\% - 100\%$, $85{,}00\% - 100\%$, dan $87{,}50\% - 98{,}44\%$. Hasil tersebut menunjukkan bahwa SHA-256 memiliki sensitivitas yang lebih konsisten terhadap perubahan data dibandingkan MD5 dan SHA-1.

Kata Kunci: Fungsi *Hash*, Integritas Data Gambar, MD5, SHA-1, SHA-256.

*Penulis Korespondensi
Info Artikel: dikirim 24 Mei 2026; direvisi 25 Juni 2026; diterima 26 Juni 2026.

1. PENDAHULUAN

Perkembangan teknologi digital menyebabkan pertukaran data elektronik semakin meningkat, termasuk penggunaan file gambar dalam berbagai kebutuhan seperti dokumentasi, komunikasi, dan penyimpanan data penting. File gambar yang disimpan maupun dikirim secara digital rentan mengalami perubahan atau manipulasi data, baik secara sengaja maupun tidak sengaja. Oleh karena itu, diperlukan suatu mekanisme untuk menjaga integritas data agar keaslian informasi tetap terjamin. Salah satu bidang ilmu yang berperan dalam pengamanan data adalah kriptografi (Lulut, dkk. 2023).

Kriptografi merupakan cabang matematika yang mempelajari teknik pengamanan informasi untuk menjaga kerahasiaan, keaslian, dan integritas data (Munir, 2004). Dalam perkembangannya, kriptografi modern dibangun berdasarkan berbagai konsep matematika diskrit seperti teori bilangan, aritmetika modular, logika boolean, dan probabilitas (Puspitasari & Mayrohmah., 2023). Konsep-konsep tersebut digunakan dalam perancangan algoritma keamanan digital, termasuk algoritma fungsi *hash*.

Fungsi *hash* merupakan algoritma matematika yang mengubah data masukan menjadi nilai ringkasan (*message digest*) dengan panjang tetap (Saputra & Nasution., 2022). Nilai *hash* yang dihasilkan memiliki karakteristik unik, yaitu perubahan kecil pada data akan menghasilkan perubahan nilai *hash* yang sangat berbeda. Sifat ini dikenal sebagai efek *avalanche* dan menjadi salah satu indikator penting dalam menilai sensitivitas serta keamanan algoritma hash (Sitorus, dkk. 2024). Selain itu, fungsi *hash* juga memiliki sifat deterministik dan resistensi terhadap kolisi sehingga banyak digunakan dalam sistem keamanan digital seperti verifikasi data, tanda tangan digital, dan teknologi *blockchain*.

Beberapa algoritma fungsi *hash* yang umum digunakan adalah MD5, SHA-1, dan SHA-256. MD5 menghasilkan nilai *hash* sepanjang 128 bit dengan proses komputasi yang relatif cepat, tetapi tingkat keamanannya lebih rendah (Zaatsiyah & Djuniadi., 2021). SHA-1 menghasilkan *message digest* sepanjang 160 bit dengan keamanan yang lebih baik dibandingkan MD5 (Santoso, dkk. 2023). Sementara itu, SHA-256 menghasilkan nilai *hash* sepanjang 256 bit dan memiliki tingkat

keamanan lebih tinggi karena lebih tahan terhadap kemungkinan kolisi (Nainggolan, 2022).

Penelitian mengenai perbandingan algoritma *hash* telah banyak dilakukan sebelumnya. Santoso dkk. (2023) membandingkan algoritma MD5 dan SHA-1 menggunakan data *username* dan *password* serta menunjukkan bahwa MD5 memiliki waktu *hashing* lebih cepat dibandingkan SHA-1. Saputra dan Nasution (2022) membandingkan algoritma MD5 dan SHA-256 pada beberapa jenis file, yaitu MP4, PDF, DOCX, MP3, dan TXT, dengan hasil bahwa MD5 lebih unggul dari sisi efisiensi waktu proses. Selain itu, Sitorus dkk. (2024) membandingkan algoritma SHA-256, SHA-3, dan Blake2 berdasarkan efek *avalanche*, ketahanan terhadap *brute force*, dan efisiensi waktu *hashing*.

Berdasarkan penelitian-penelitian tersebut, objek pengujian yang digunakan meliputi data *username* dan *password* serta berbagai jenis file seperti dokumen, dan teks. Pada penelitian ini, file gambar digunakan sebagai objek pengujian karena merupakan salah satu bentuk data digital yang paling sering digunakan dalam kehidupan sehari-hari, baik sebagai media identitas, dokumentasi, maupun penyimpanan informasi. Dalam penggunaannya, file gambar sering mengalami berbagai proses pengolahan, seperti kompresi, pengeditan, atau perubahan kecil pada gambar. Meskipun perubahan tersebut terkadang tidak terlihat secara visual, struktur data file dapat mengalami perubahan yang mengakibatkan nilai *hash* yang dihasilkan menjadi berbeda. Oleh karena itu, penelitian ini dilakukan untuk membandingkan kemampuan algoritma MD5, SHA-1, dan SHA-256 dalam mendeteksi perubahan pada file gambar serta menjaga integritas data yang terkandung di dalamnya.

2. METODE PENELITIAN

Penelitian ini merupakan penelitian eksperimen komputasi yang bertujuan untuk menganalisis kemampuan algoritma *hash* MD5, SHA-1, dan SHA-256 dalam menjaga integritas data pada file gambar digital. Objek penelitian berupa file gambar e-Kartu Tanda Mahasiswa (e-KTM), yaitu kartu identitas mahasiswa dalam format digital yang digunakan sebagai bukti status kemahasiswaan dan memuat informasi penting seperti nama mahasiswa, nomor induk mahasiswa, program

studi, serta foto mahasiswa. Data yang digunakan merupakan file e-KTM mahasiswa Program Studi Matematika FMIPA Universitas Mulawarman dengan format JPG. Pengujian dilakukan dengan membandingkan nilai *hash* file gambar asli dengan nilai *hash* file yang telah dimodifikasi melalui proses kompresi serta perubahan satu piksel. Seluruh proses dilakukan menggunakan bahasa pemrograman Python dengan pustaka *hashlib*.

2.1 Fungsi *Hash*

Fungsi *hash* kriptografi merupakan fungsi satu arah yang mengubah data masukan menjadi nilai *hash* dengan panjang tetap (Munir, 2004). Secara matematis fungsi *hash* dinyatakan sebagai.

$$h = H(m) \tag{1}$$

dengan m menyatakan data masukan, H menyatakan fungsi *hash*, dan h menyatakan nilai *hash* yang dihasilkan. Pada penelitian ini digunakan algoritma MD5, SHA-1, dan SHA-256 untuk menghasilkan nilai *hash* file gambar.

2.2 Algoritma MD5

Message Digest 5 (MD5) merupakan algoritma *hash* yang menghasilkan nilai *hash* sepanjang 128 bit. Algoritma ini menggunakan fungsi nonlinier berbasis operasi bitwise, yaitu

$$\begin{aligned} F(b_t, c_t, d_t) &= (b_t \wedge c_t) \vee (\neg b_t \wedge d_t), \\ G(b_t, c_t, d_t) &= (b_t \wedge d_t) \vee (c_t \wedge \neg d_t), \\ H(b_t, c_t, d_t) &= b_t \oplus c_t \oplus d_t, \\ I(b_t, c_t, d_t) &= c_t \oplus (b_t \wedge \neg d_t) \end{aligned} \tag{2}$$

dengan F, G, H, dan I merupakan fungsi nonlinier yang digunakan pada setiap putaran MD5, dan b_t, c_t, dan $d_t$adalah nilai *buffer* pada iterasi ke-t.

Proses kompresi MD5 dilakukan menggunakan persamaan

$$a_{t+1} = b_t + ((a_t + g(b_t, c_t, d_t) + W[k] + T[i]) \lll s) \tag{3}$$

Dengan g menyatakan fungsi nonlinier MD5, $W[k]$ merupakan blok pesan, $T[i]$ merupakan konstanta iterasi dan $\lll$ menyatakan operasi rotasi bit ke kiri (Munir, 2019).

2.3 Algoritma SHA-1

Secure Hash Algorithm-1 (SHA-1) merupakan algoritma *hash* yang menghasilkan nilai *hash* sepanjang 160 bit. Pembentukan *message schedule* dilakukan menggunakan persamaan.

$$W_t = (W_{t-3} \oplus W_{t-8} \oplus W_{t-14} \oplus W_t - 16) \lll 1 \quad (4)$$

Sedangkan proses kompresi SHA-1 dihitung menggunakan persamaan

$$T_{t+1} = (a_t) \lll 5) + f_t \ (b_t, c_t, d_t) + e_t \ + K_t \ + W_t \quad (5)$$

dengan f_t menyatakan fungsi logika SHA-1, K_t merupakan konstanta putaran, dan W_t merupakan hasil ekspansi pesan (Sari, 2024).

2.4 Algoritma SHA-256

Secure Hash Algorithm-256 (SHA-256) merupakan algoritma *hash* yang menghasilkan nilai *hash* sepanjang 256 bit. Proses ekspansi pesan dilakukan menggunakan persamaan

$$W_t = \sigma_1(W_{t-2}) + W_{t-7} + \sigma_0(W_{t-15}) + W_{t-16} \quad (6)$$

dengan fungsi

$$\sigma_0(x) = (x \ggg 7) \oplus (x \ggg 18) \oplus (x \gg 3)$$
$$\sigma_1(x) = (x \ggg 17) \oplus (x \ggg 19) \oplus (x \gg 10) \quad (7)$$

dengan W_t menyatakan kata (*word*) ke-t hasil ekspansi pesan, σ_0 dan σ_1 merupakan fungsi transformasi yang digunakan dalam proses *message schedule*, sedangkan $\ggg$ menyatakan operasi rotasi bit ke kanan dan $\gg$ menyatakan operasi pergeseran bit ke kanan.

Selanjutnya proses putaran SHA-256 dihitung menggunakan persamaan

$$T_1 = h_t + \Sigma_1(e_t) + Ch(e_t, f_t, g_t) + K_t + W_t$$
$$T_2 = \Sigma_0(a_t) + Maj(a_t, b_t, c_t) \quad (8)$$

dengan Ch menyatakan fungsi *choice*, Majmenyatakan fungsi mayoritas bit (*majority*), Σ_0 dan $\Sigma_1$merupakan fungsi transformasi pada proses kompresi SHA-256, K_t merupakan konstanta putaran ke-t, a_t, b_t, c_t, e_t, f_t, g_t, dan $h_t$merupakan nilai *buffer* SHA-256 pada iterasi ke-t, serta T_1 dan T_2 merupakan nilai sementara yang digunakan dalam proses kompresi (Nainggolan, 2022).

2.5 Efek *Avalanche*

Sensitivitas algoritma *hash* terhadap perubahan data diukur menggunakan efek *avalanche*. Efek *avalanche* dihitung menggunakan persamaan

$$AE = \frac{jumlah\ heksadesimal\ berbeda}{total\ heksadesimal} \times 100\% \quad (9)$$

Semakin besar nilai efek *avalanche*, maka semakin baik kemampuan algoritma dalam mendeteksi perubahan kecil pada data (Karima, dkk., 2024).

2.6 Prosedur Pengujian

Pengujian dimulai dengan menghitung nilai *hash* file gambar asli menggunakan algoritma MD5, SHA-1, dan SHA-256. Selanjutnya dilakukan modifikasi file gambar melalui kompresi dan perubahan satu piksel. File hasil modifikasi kemudian diproses kembali menggunakan ketiga algoritma *hash* untuk memperoleh nilai *hash* baru.

Nilai hash file asli dan file hasil modifikasi dibandingkan untuk menguji integritas data. Selanjutnya dilakukan perhitungan efek *avalanche* untuk mengetahui sensitivitas algoritma terhadap perubahan kecil pada data. Tahap akhir dilakukan dengan menganalisis hasil pengujian untuk menentukan algoritma *hash* yang paling efektif dalam menjaga integritas file gambar.

3. HASIL DAN PEMBAHASAN

Pada penelitian ini dilakukan perbandingan tiga algoritma fungsi *hash*, yaitu MD5, SHA 1, dan SHA-256, dalam menjaga integritas file gambar. Data yang digunakan berupa 30 file gambar e-KTM mahasiswa Program Studi S-1 Matematika FMIPA Universitas Mulawarman berformat JPG. Setiap file diproses menggunakan ketiga algoritma untuk menghasilkan nilai *hash*, kemudian dilakukan pengujian integritas melalui perubahan satu piksel dan kompresi file. Parameter yang dianalisis meliputi panjang nilai *hash*, waktu proses *hashing*, efek *avalanche*, dan kemampuan mendeteksi perubahan data.

Hasil pengujian menunjukkan bahwa ketiga algoritma menghasilkan nilai *hash* dengan panjang tetap sesuai karakteristik masing-masing. MD5 menghasilkan *hash* sepanjang 128 bit, SHA-1 sepanjang 160 bit, dan SHA-256 sepanjang 256 bit. Perbedaan panjang luaran ini menunjukkan bahwa SHA-256 memiliki ruang

kemungkinan nilai *hash* yang lebih besar, sehingga secara teoritis memiliki ketahanan yang lebih baik terhadap kemungkinan kolisi.

Berdasarkan pengujian terhadap 30 file gambar, seluruh algoritma menghasilkan nilai *hash* yang berbeda untuk setiap file dan tidak ditemukan kolisi. Selain itu, hasil pengujian waktu proses menunjukkan bahwa MD5 memiliki waktu komputasi paling cepat, diikuti oleh SHA-1, sedangkan SHA-256 memiliki struktur perhitungan yang lebih kompleks.

Tabel 1. Perbandingan Karakteristik Algoritma Hashing.

Algoritma	Panjang Hash	Waktu Proses (detik)	Kolisi
MD5	128 bit	0.000036–0.001379	Tidak ditemukan
SHA-1	160 bit	0.000077–0.001843	Tidak ditemukan
SHA-256	256 bit	0.000037–0.001241	Tidak ditemukan

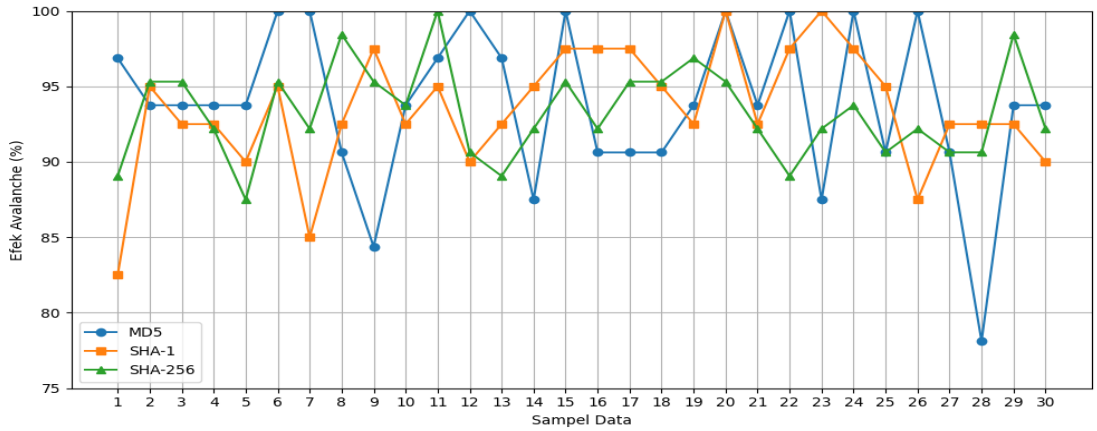
Berdasarkan Tabel 1, MD5 merupakan algoritma yang paling efisien dari sisi waktu komputasi, sedangkan SHA-256 memiliki keunggulan dari sisi panjang luaran *hash* dan kompleksitas algoritma yang lebih tinggi. Hal ini menunjukkan adanya *trade-off* antara efisiensi komputasi dan tingkat keamanan.

3.1 Uji Integritas dengan Perubahan File

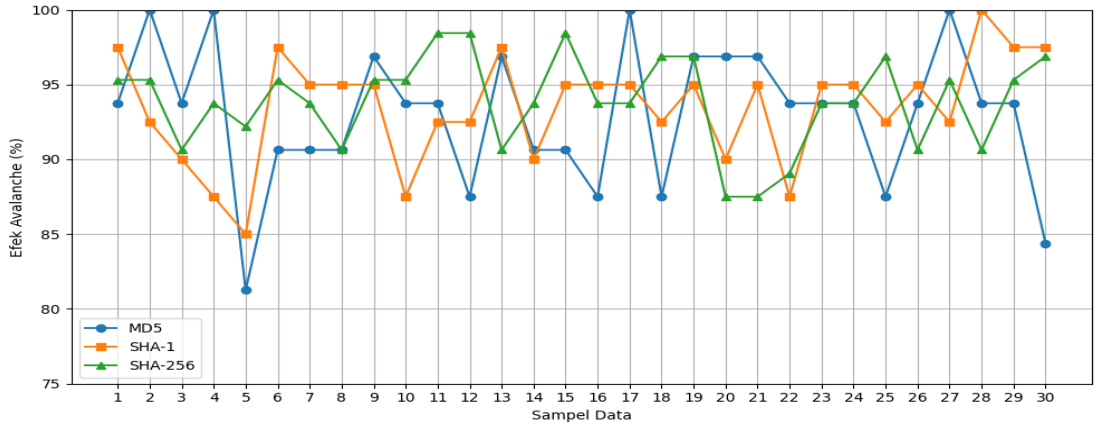
Pengujian integritas dilakukan melalui dua perlakuan, yaitu perubahan satu piksel dan kompresi file gambar. Hasil pengujian menunjukkan bahwa seluruh nilai *hash* berubah setelah file dimodifikasi. Meskipun perubahan satu piksel hampir tidak terlihat secara visual, perubahan tersebut tetap menghasilkan nilai *hash* yang berbeda secara keseluruhan. Demikian pula, kompresi file yang tidak mengubah tampilan gambar secara signifikan tetap memengaruhi struktur data internal file sehingga menghasilkan nilai hash yang berbeda.

Hasil ini menunjukkan bahwa ketiga algoritma memiliki sensitivitas yang tinggi terhadap perubahan data dan mampu digunakan sebagai mekanisme verifikasi integritas file gambar. Untuk mengukur tingkat sensitivitas algoritma secara kuantitatif, digunakan parameter efek avalanche yang dihitung menggunakan Persamaan (24). Efek *avalanche* menunjukkan persentase perubahan karakter heksadesimal pada nilai hash akibat perubahan kecil pada data masukan. Semakin tinggi nilai efek *avalanche*, semakin baik kemampuan algoritma dalam mendeteksi perubahan data.

Hasil pengujian terhadap 30 file gambar divisualisasikan pada Gambar 1 dan Gambar 2.



Gambar 1. Grafik Perbandingan Efek *Avalanche* pada Perubahan Satu Piksel



Gambar2. Grafik Perbandingan Efek *Avalanche* pada Perubahan Kompresi File

Berdasarkan Gambar 1 dan Gambar 2, nilai efek *avalanche* yang dihasilkan oleh algoritma MD5, SHA-1, dan SHA-256 pada seluruh sampel berada pada rentang yang tinggi. Pada perlakuan perubahan satu piksel maupun kompresi file, ketiga algoritma menunjukkan perubahan nilai hash yang signifikan meskipun perubahan yang dilakukan pada file relatif kecil. Hal ini menunjukkan bahwa seluruh algoritma memiliki sensitivitas yang baik dalam mendeteksi perubahan data.

Pada perlakuan perubahan satu piksel, nilai efek *avalanche* MD5 berada pada rentang 78,13% hingga 100%, SHA-1 berada pada rentang 82,50% hingga 100%, sedangkan SHA-256 berada pada rentang 87,50% hingga 100%. Sementara itu, pada perlakuan kompresi file, nilai efek avalanche MD5 berada pada

rentang 81,25% hingga 100%, SHA-1 berada pada rentang 85,00% hingga 100%, dan SHA-256 berada pada rentang 87,50% hingga 98,44%.

Secara umum, SHA-256 menunjukkan nilai efek *avalanche* yang lebih stabil dengan rentang nilai minimum yang relatif lebih tinggi dibandingkan MD5 dan SHA-1. Hal ini mengindikasikan bahwa SHA-256 memiliki sensitivitas yang lebih konsisten terhadap perubahan data. Di sisi lain, MD5 dan SHA-1 juga mampu menghasilkan efek avalanche yang tinggi, namun masih menunjukkan variasi nilai yang lebih besar pada beberapa sampel. Dengan demikian, ketiga algoritma mampu digunakan untuk verifikasi integritas file gambar, tetapi SHA-256 memberikan performa yang lebih baik dari sisi sensitivitas terhadap perubahan data.

Tabel 2. Ringkasan Hasil Uji Integritas Algoritma Hashing Berdasarkan Efek Avalanche

Algoritma	Perlakuan	Rentang Efek *Avalanche* (%)
MD5	Kompresi	$81.25 - 100$
	Perubahan 1 Piksel	$78.13 - 100$
SHA-1	Kompresi	$85.00 - 100$
	Perubahan 1 Piksel	$82.50 - 100$
SHA-256	Kompresi	$87.50 - 98.44$
	Perubahan 1 Piksel	$87.50 - 100$

Berdasarkan Tabel 2, seluruh algoritma mampu mendeteksi perubahan data dengan sangat baik. Namun, SHA-256 menunjukkan sensitivitas paling tinggi karena memiliki nilai efek *avalanche* yang lebih stabil dan nilai minimum yang lebih besar dibandingkan algoritma lainnya.

3.2 Uji Integritas dengan Perubahan File

Dari sisi keamanan, panjang luaran *hash* memengaruhi besar ruang kemungkinan nilai yang dapat dihasilkan. MD5 memiliki ruang nilai sebesar 2^{128}, SHA-1 sebesar 2^{160}, dan SHA-256 sebesar 2^{256}. Semakin besar ruang nilai tersebut, semakin kecil probabilitas terjadinya kolisi.

Dari sisi efisiensi, MD5 merupakan algoritma tercepat, sedangkan SHA-256 memberikan tingkat keamanan tertinggi. Oleh karena itu, pemilihan algoritma perlu mempertimbangkan keseimbangan antara kecepatan dan tingkat keamanan yang dibutuhkan.

Tabel 3. Ringkasan Hasil Uji Integritas Algoritma Hashing Berdasarkan Efek *Avalanche*

Algoritma	Rentang Efek Avalanche Ubah 1 Piksel (%)	Rentang Efek Avalanche Kompresi File (%)	Waktu Proses (detik) [min–maks]	Evaluasi Keamanan dan Efisiensi
MD5	78,13% – 100%	81,25% – 100%	0.000036–0.001379	Memiliki waktu komputasi paling cepat dan mampu mendeteksi perubahan data dengan baik. Namun, panjang hash yang lebih pendek menyebabkan tingkat ketahanan terhadap kolisi lebih rendah dibandingkan algoritma lainnya.
SHA-1	82,50% – 100%	85,00% – 100%	0.000077–0.001843	Menunjukkan sensitivitas yang baik terhadap perubahan data dengan tingkat keamanan yang lebih tinggi dibandingkan MD5. Namun, keamanan yang dihasilkan masih berada di bawah SHA-256.
SHA-256	87,50% – 100%	87,50% – 98,44%	0.000037–0.001241	Memiliki rentang efek *avalanche* yang tinggi dan lebih stabil, serta panjang *hash* yang lebih besar sehingga memberikan tingkat keamanan yang lebih baik dalam menjaga integritas data.

Berdasarkan Tabel 3, SHA-256 merupakan algoritma terbaik dalam penelitian ini karena memiliki panjang hash paling besar, nilai efek *avalanche* tertinggi, dan kemampuan paling konsisten dalam mendeteksi perubahan data. MD5 tetap unggul dari sisi kecepatan, tetapi tingkat keamanannya lebih rendah. Oleh karena itu, SHA-256 direkomendasikan sebagai algoritma yang paling efektif untuk menjaga integritas file gambar.

4. KESIMPULAN DAN SARAN

Berdasarkan hasil penelitian, algoritma *hash* MD5, SHA-1, dan SHA-256 dapat digunakan untuk menjaga integritas file gambar berformat JPG. Hasil pengujian menunjukkan bahwa perubahan satu piksel maupun kompresi file menghasilkan nilai hash yang berbeda sehingga ketiga algoritma mampu mendeteksi perubahan data dengan baik. Nilai efek *avalanche* yang diperoleh pada

seluruh pengujian berada pada rentang yang tinggi. Pada perlakuan perubahan satu piksel, nilai efek *avalanche* MD5 berada pada rentang $78{,}13\% - 100\%$, SHA-1 berada pada rentang $82{,}50\% - 100\%$, dan SHA-256 berada pada rentang $87{,}50\% - 100\%$. Pada perlakuan kompresi file, nilai efek *avalanche* MD5 berada pada rentang $81{,}25\% - 100\%$, SHA-1 berada pada rentang $85{,}00\% - 100\%$, dan SHA-256 berada pada rentang $87{,}50\% - 98{,}44\%$. Hasil tersebut menunjukkan bahwa ketiga algoritma memiliki sensitivitas yang baik terhadap perubahan data.

Dari ketiga algoritma yang diuji, SHA-256 menunjukkan sensitivitas yang lebih baik dengan nilai efek *avalanche* minimum yang lebih tinggi serta ruang kemungkinan *hash* yang lebih luas, sehingga lebih tahan terhadap kolisi. Oleh karena itu, SHA-256 dinilai lebih sesuai untuk menjaga integritas file gambar. Penelitian selanjutnya dapat menggunakan lebih banyak sampel dan membandingkan algoritma *hash* lainnya untuk memperoleh hasil yang lebih komprehensif.

DAFTAR PUSTAKA

Karima, N.A., Aisyah, A.N., Silla, H.V., Handoko, L.B., dan Sani, R.R., *Kriptografi Teks Berbasis Algoritma Substitusi Vigenere Cipher 8 Bit*, Jurnal Masyarakat Informatika, **15**(1) (2024).

Lulut, A., Khairunnisa, F.R., Mindo., Ida, F.A., Suwito, P., Indah, R.A.S., dan Wirawan, I., *Handbook of Applied Cryptography*, CRC Press, New York, 2023.

Munir, R., *Kriptografi*, Informatika Bandung, Bandung, 2019.

Munir, R., *Pengantar Kriptografi*, Departemen Teknik Informatika Institut Teknologi Bandung, Bandung, 2004.

Nainggolan, S., *Implementasi Algoritma SHA-256 Pada Aplikasi Duplicate Document Scanner*, RESOLUSI: Rekayasa Teknik Informatika dan Informasi, **2**(5) (2022), 201–213.

National Institute of Standards and Technology, Secure Hash Standard (SHS), FIPS PUB 180-4, 2015.

Permana, A.A. dan Nurnaningsih, D., *Rancangan Aplikasi Pengamanan Data dengan Algoritma Advanced Encryption Standard (AES)*, Jurnal Teknik Informatika, **11**(2) (2018), 177–186.

Puspitasari, N. dan Mayrohmah, S.H., *Peran Aljabar Boolean dalam Ilmu Komputer dan Perancangan Rangkaian Logika*, Jurnal Informa: Jurnal Penelitian dan Pengabdian Masyarakat, **9**(2) (2023), 26–33.

Sari, N.H., *Penerapan Teknik Digital Signature dalam Pengamanan Piagam Penghargaan Menggunakan Algoritma SHA-1 dan RSA*, Management of Information System Journal, **2**(3) (2024), 55–67.

Santoso, M.H., Girsang, N.D., Siagian, H., Wahyudi, A., dan Sitorus, B.A., *Perbandingan Algoritma Kriptografi Hash MD5 dan SHA-1*, Prosiding Seminar Nasional Teknologi Informatika, **1**(1) (2023), 54–58.

Saputra, I. dan Nasution, S.D., *Perbandingan Performa Algoritma MD5 dan SHA-256 dalam Membangkitkan Identitas File*, Jurnal Sains Komputer & Informatika (J-SAKTI), **6**(1) (2022), 172–187.

Sitorus, N., Gabriella, J.S., Sinaga, dan Samosir, S.L., *Analisis Kinerja Algoritma Hash pada Keamanan Data: Perbandingan Antara SHA-256, SHA-3, dan Blake2*, Jurnal Quancoma, **2**(2) (2024), 9–16.

Zaatsiyah, N. dan Djuniadi, *Implementing Digital Signature with RSA and MD5 in Securing E-Invoice Document*, Jurnal Pendidikan Teknologi Informasi, **5**(2) (2021), 129–140.