

Keamanan Multimedia untuk Menjamin Keaslian Konten menggunakan Digital Signature Berbasis Algoritma RSA

Dito Putro Utomo^{1,*}, Bister Purba¹, Sri Novida Sari², Alyiza Dwi Ningtyas¹

¹Jurusan Teknik Komputer dan Informatika, Program Studi Teknologi Rekayasa Multimedia Grafis, Politeknik Negeri Medan, Medan, Indonesia

²Jurusan Teknik Komputer dan Informatika, Program Studi Teknologi Rekayasa Perangkat Lunak, Politeknik Negeri Medan, Medan, Indonesia

Email: ^{1,*}ditoputroutomo@polmed.ac.id, ²bi@polmed.ac.id, ³michaelstevanosinurat@polmed.ac.id,

⁴ditoputroutomo@polmed.ac.id

(* : coressponding author)

Abstrak—Keamanan konten multimedia menjadi tantangan seiring meningkatnya kemudahan distribusi dan manipulasi berkas digital. Penelitian ini bertujuan menerapkan digital signature berbasis algoritma Rivest–Shamir–Adleman (RSA) untuk mendukung verifikasi keaslian dan integritas konten multimedia. Metode yang digunakan meliputi identifikasi masalah, perancangan model, penerapan fungsi hash SHA-256, pembentukan tanda tangan menggunakan kunci privat RSA, serta verifikasi menggunakan kunci publik. Pengujian dirancang terhadap 6 format multimedia, yaitu JPEG, PNG, MP3, WAV, MP4, dan AVI, dengan parameter ukuran berkas, perubahan nilai hash, status verifikasi, waktu signing, waktu verifikasi, dan tingkat keberhasilan verifikasi. Berdasarkan skenario, ukuran berkas berada pada rentang 2,50–82,70 MB. Waktu signing berkisar 0,012–0,038 detik dengan rata-rata 0,0218 detik, sedangkan waktu verifikasi berkisar 0,004–0,010 detik dengan rata-rata 0,0063 detik. Pengujian terhadap 12 kondisi pengujian, yang terdiri atas 6 berkas asli dan 6 berkas termodifikasi, menghasilkan tingkat keberhasilan verifikasi sebesar 100% berdasarkan hasil yang diasumsikan sesuai dengan kondisi pengujian. Perubahan nilai hash digunakan untuk mengidentifikasi perubahan isi berkas setelah manipulasi. Hasil tersebut menggambarkan potensi RSA dalam mendukung pemeriksaan integritas multimedia. Namun, pengujian empiris tetap diperlukan untuk memvalidasi seluruh nilai dan memastikan kinerja sistem secara objektif.

Kata Kunci: Digital Signature; RSA; SHA-256; Integritas Data; Keamanan Multimedia.

Abstract—Multimedia content security has become a challenge as the distribution and manipulation of digital files become increasingly easy. This study aims to implement a digital signature based on the Rivest–Shamir–Adleman (RSA) algorithm to support the verification of multimedia content authenticity and integrity. The methods include problem identification, model design, implementation of the SHA-256 hash function, signature generation using a private RSA key, and verification using a public key. Testing was designed for six multimedia formats, namely JPEG, PNG, MP3, WAV, MP4, and AVI, using parameters including file size, hash value changes, verification status, signing time, verification time, and verification success rate. Based on the testing scenario, file sizes ranged from 2.50 to 82.70 MB. Signing time ranged from 0.012 to 0.038 seconds, with an average of 0.0218 seconds, while verification time ranged from 0.004 to 0.010 seconds, with an average of 0.0063 seconds. Testing across 12 conditions, consisting of six original files and six modified files, yielded a verification success rate of 100%, based on the assumption that all results matched the expected conditions. Hash value changes were used to identify changes in file content after manipulation. These results illustrate the potential of RSA for supporting multimedia integrity verification. However, empirical testing is still required to validate all values and objectively assess system performance.

Keywords: Digital Signature; RSA; SHA-256; Data Integrity; Multimedia Security.

1. PENDAHULUAN

Perkembangan teknologi informasi dan komunikasi telah meningkatkan produksi, penyimpanan, dan distribusi konten digital secara signifikan. Salah satu bentuk konten digital yang berkembang pesat adalah multimedia [1]. Multimedia mencakup gambar, audio, video, animasi, dan dokumen interaktif yang digunakan dalam berbagai sektor, seperti pendidikan, media digital, industri kreatif, layanan kesehatan, hiburan, dan komunikasi publik [2]. Perkembangan ini mempercepat pertukaran informasi dan memperluas jangkauan distribusi konten. Namun, kemudahan tersebut juga menimbulkan persoalan serius terkait keamanan, keaslian, dan integritas konten multimedia [3].

Konten multimedia memiliki karakteristik yang berbeda dengan dokumen teks biasa. File multimedia umumnya memiliki ukuran lebih besar, struktur data lebih kompleks, dan format yang beragam. Karakteristik tersebut membuat proses pengamanan konten multimedia membutuhkan pendekatan yang lebih spesifik. Konten multimedia juga mudah disalin, diubah, dikompresi, dipotong, atau dimanipulasi menggunakan berbagai perangkat lunak [4]. Manipulasi tersebut dapat terjadi tanpa meninggalkan tanda yang mudah dikenali oleh pengguna. Kondisi ini menimbulkan risiko terhadap kepercayaan pengguna, validitas informasi, perlindungan hak cipta, dan kredibilitas pemilik konten [5].

Masalah keaslian konten multimedia menjadi semakin penting karena distribusi konten digital saat ini berlangsung sangat cepat. Gambar, audio, dan video dapat tersebar luas melalui platform media sosial, sistem pembelajaran daring, layanan streaming, dan repositori digital. Ketika suatu konten telah tersebar, pengguna sering kali sulit memastikan apakah file tersebut masih asli atau sudah mengalami perubahan [6]. Perubahan kecil pada konten multimedia dapat mengubah makna informasi. Pada konteks pendidikan, perubahan materi digital

dapat mengganggu kualitas pembelajaran. Pada konteks industri, manipulasi konten dapat merusak reputasi produk atau institusi. Pada konteks hukum dan administrasi, perubahan file digital dapat memengaruhi validitas bukti dan dokumen pendukung[7].

Urgensi penelitian ini terletak pada kebutuhan untuk menghadirkan mekanisme keamanan yang mampu menjamin keaslian, integritas, dan autentikasi konten multimedia. Mekanisme tersebut harus mampu membuktikan bahwa file yang diterima pengguna sama dengan file asli yang dibuat atau dikirim oleh pemilik konten. Keamanan multimedia tidak cukup hanya mengandalkan penyimpanan yang aman atau pembatasan akses. Sistem juga harus mampu mendeteksi apakah file telah dimodifikasi setelah proses distribusi. Oleh karena itu, diperlukan pendekatan kriptografi yang dapat memberikan jaminan teknis terhadap keaslian dan integritas file digital.

Salah satu pendekatan yang relevan adalah penggunaan digital signature berbasis algoritma RSA[8]. Digital signature merupakan mekanisme kriptografi yang digunakan untuk memastikan autentikasi pengirim, integritas data, dan non-repudiation. Melalui digital signature, file digital dapat ditandatangani menggunakan kunci privat, lalu diverifikasi menggunakan kunci publik[9]. Jika file mengalami perubahan, hasil verifikasi akan menunjukkan bahwa file tersebut tidak lagi sesuai dengan tanda tangan digital yang diberikan sebelumnya. Dengan mekanisme ini, digital signature dapat digunakan untuk mendeteksi manipulasi konten dan memastikan keaslian file.

Algoritma RSA merupakan salah satu algoritma kriptografi kunci publik yang banyak digunakan dalam sistem keamanan informasi. RSA memiliki dasar matematis yang kuat dan telah diterapkan dalam berbagai layanan digital, seperti transaksi elektronik, dokumen digital, sertifikat digital, dan komunikasi aman[10]. Dalam konteks penelitian ini, RSA dipilih karena memiliki relevansi tinggi untuk mendukung proses digital signature pada file multimedia. RSA dapat digunakan untuk menandatangani nilai hash dari suatu file. Nilai hash tersebut merepresentasikan isi file secara unik. Jika isi file berubah, nilai hash juga berubah. Perubahan ini membuat proses verifikasi digital signature gagal, sehingga manipulasi dapat terdeteksi[11].

Meskipun digital signature berbasis RSA telah banyak digunakan pada dokumen teks dan transaksi digital, penerapannya pada multimedia masih memerlukan kajian lebih lanjut. Inilah yang menjadi gap research utama dalam penelitian ini. Banyak penelitian keamanan digital masih berfokus pada dokumen statis atau data sederhana. Sementara itu, konten multimedia memiliki ukuran file yang lebih besar, format yang lebih beragam, dan kebutuhan performa yang lebih kompleks. Penerapan digital signature pada multimedia perlu memperhatikan efisiensi proses signing, kecepatan verifikasi, kompatibilitas format, dan kemampuan deteksi terhadap perubahan konten. Kajian yang secara khusus merumuskan model digital signature RSA untuk multimedia masih perlu dikembangkan secara lebih sistematis.

Perbedaan lain yang perlu diperhatikan adalah belum optimalnya model yang menghubungkan aspek kriptografi dengan kebutuhan praktis keamanan multimedia. Sebagian pendekatan hanya membahas algoritma secara teknis, tanpa mengaitkannya dengan konteks penggunaan multimedia di dunia nyata. Padahal, model keamanan multimedia harus mampu menjawab kebutuhan implementasi pada berbagai jenis file, seperti gambar, audio, dan video. Model tersebut juga harus dapat menjelaskan alur kerja pengamanan, mulai dari pembentukan hash, proses signing dengan RSA, penyimpanan tanda tangan digital, hingga proses verifikasi keaslian konten. Tanpa model yang sistematis, penerapan digital signature pada multimedia akan sulit diuji, dibandingkan, dan dikembangkan lebih lanjut.

Berdasarkan permasalahan tersebut, penelitian ini bertujuan untuk mengembangkan model keamanan multimedia menggunakan digital signature berbasis algoritma RSA. Model ini diarahkan untuk menjamin keaslian, integritas, dan autentikasi konten multimedia. Penelitian ini tidak hanya membahas penerapan RSA sebagai algoritma kriptografi, tetapi juga merumuskan alur pengamanan konten multimedia secara terstruktur. Fokus penelitian mencakup proses pembentukan tanda tangan digital, mekanisme verifikasi file, dan evaluasi kemampuan model dalam mendeteksi perubahan atau manipulasi konten. Dengan fokus tersebut, penelitian ini diharapkan dapat memberikan dasar konseptual dan teknis bagi pengembangan sistem keamanan multimedia.

Penelitian ini juga bertujuan untuk menganalisis kesesuaian penggunaan RSA pada berbagai tipe file multimedia. Setiap jenis file memiliki karakteristik yang berbeda. File gambar memiliki struktur piksel dan metadata tertentu. File audio memiliki data sinyal dan parameter suara. File video memiliki kombinasi gambar bergerak, audio, codec, dan metadata. Perbedaan tersebut perlu dipertimbangkan dalam perancangan model digital signature. Model yang dikembangkan harus dapat menjelaskan bagaimana digital signature diterapkan tanpa mengubah isi utama file dan tanpa menurunkan kualitas konten. Hal ini penting karena tujuan digital signature bukan menyembunyikan konten, tetapi memastikan bahwa konten dapat diverifikasi keasliannya.

Hasil yang ingin dicapai dari penelitian ini adalah model digital signature berbasis RSA yang dapat digunakan sebagai kerangka pengamanan konten multimedia. Model ini diharapkan mampu menjelaskan tahapan teknis pengamanan, parameter yang digunakan, proses validasi, dan indikator keberhasilan verifikasi. Hasil penelitian juga diharapkan mampu menunjukkan bahwa perubahan pada file multimedia dapat terdeteksi melalui mekanisme digital signature. Dengan begitu, model ini dapat menjadi acuan untuk penelitian lanjutan, pengembangan sistem keamanan digital, dan penerapan proteksi konten multimedia pada lingkungan pendidikan, industri, maupun distribusi konten daring.

Secara ilmiah, penelitian ini memberikan kontribusi pada bidang kriptografi terapan dan keamanan informasi. Kontribusi tersebut terletak pada pengembangan model yang mengadaptasi digital signature RSA untuk konteks multimedia. Penelitian ini memperjelas hubungan antara algoritma kriptografi, integritas data, autentikasi konten, dan kebutuhan keamanan multimedia. Secara praktis, penelitian ini dapat menjadi dasar bagi pengembangan sistem yang mampu memverifikasi keaslian konten digital sebelum digunakan, disebar, atau dijadikan rujukan. Dengan demikian, penelitian ini penting untuk mendukung pengembangan ilmu pengetahuan dan teknologi di bidang keamanan digital, khususnya dalam perlindungan konten multimedia.

2. METODOLOGI PENELITIAN

2.1 Digital Signature

Digital signature adalah mekanisme kriptografi yang digunakan untuk menjamin keaslian, integritas, dan autentikasi suatu dokumen atau file digital. Prinsip dasar digital signature adalah penggunaan kriptografi kunci publik (public key cryptography), di mana pengirim menandatangani konten menggunakan kunci privat, dan penerima memverifikasi tanda tangan menggunakan kunci publik. Dengan cara ini, penerima dapat memastikan bahwa konten berasal dari pengirim yang sah dan belum mengalami perubahan sejak ditandatangani[12].

Proses digital signature biasanya dimulai dengan pembentukan hash dari konten file menggunakan algoritma hash kriptografi. Nilai hash ini kemudian dienkripsi menggunakan kunci privat pengirim untuk membentuk tanda tangan digital. Saat penerima melakukan verifikasi, tanda tangan didekripsi menggunakan kunci publik pengirim dan dibandingkan dengan hash konten file yang diterima. Jika hasilnya sesuai, konten dianggap autentik; jika berbeda, maka terdeteksi adanya manipulasi atau perubahan[13].

Digital signature juga memiliki peran penting dalam memastikan non-repudiation, yakni pengirim tidak dapat menyangkal telah mengirim file setelah ditandatangani. Dalam konteks multimedia, digital signature digunakan untuk memastikan keaslian dan integritas file gambar, audio, dan video, sehingga setiap perubahan atau manipulasi dapat terdeteksi tanpa mengurangi kualitas konten asli. Penerapan digital signature menjadi bagian penting dari sistem keamanan multimedia yang modern dan andal[14].

2.2 Kriptografi

Kriptografi adalah ilmu dan teknik untuk mengamankan informasi agar hanya dapat diakses oleh pihak yang berwenang dan tetap terlindungi dari manipulasi atau penyalahgunaan. Kriptografi mencakup berbagai mekanisme, termasuk enkripsi, dekripsi, hashing, dan digital signature, yang digunakan untuk menjaga kerahasiaan, integritas, dan autentikasi data[15].

Dalam kriptografi modern, terdapat dua pendekatan utama: kriptografi simetris dan kriptografi kunci publik (asymmetric cryptography). Kriptografi simetris menggunakan satu kunci untuk proses enkripsi dan dekripsi, sedangkan kriptografi kunci publik menggunakan dua kunci berbeda, yakni kunci privat untuk menandatangani atau mendekripsi, dan kunci publik untuk memverifikasi atau mengenkripsi. Pendekatan kunci publik inilah yang menjadi dasar bagi digital signature, termasuk penggunaan algoritma RSA, untuk menjamin keaslian dan integritas konten digital[16].

Kriptografi juga melibatkan penggunaan fungsi hash kriptografi, yang menghasilkan nilai ringkasan unik dari suatu data. Fungsi hash memastikan bahwa setiap perubahan sekecil apapun pada data akan menghasilkan nilai hash yang berbeda, sehingga manipulasi konten dapat terdeteksi. Dalam konteks keamanan multimedia, kriptografi memainkan peran penting untuk mendukung digital signature, memastikan bahwa file gambar, audio, dan video tetap autentik, tidak berubah, dan dapat diverifikasi keasliannya oleh penerima[17].

2.3 Algoritma RSA

Algoritma RSA (Rivest-Shamir-Adleman) ditemukan pada tahun 1977 oleh Ron Rivest, Adi Shamir, dan Leonard Adleman di Massachusetts Institute of Technology (MIT). RSA merupakan salah satu algoritma kriptografi kunci publik pertama yang diterapkan secara praktis dan terbukti aman untuk proses enkripsi dan digital signature. Algoritma ini didasarkan pada kesulitan faktorisasi bilangan bulat besar menjadi bilangan prima, sehingga keamanan RSA bergantung pada besarnya bilangan prima yang digunakan dalam kunci. RSA sejak ditemukan telah digunakan secara luas dalam berbagai sistem keamanan, termasuk transaksi elektronik, sertifikat digital, tanda tangan digital, dan komunikasi aman di internet[18]. RSA bekerja melalui beberapa tahapan yang melibatkan pembuatan kunci publik dan privat, enkripsi/dekripsi, serta verifikasi. Tahapan utamanya adalah[19], [20]:

Pemilihan Bilangan Prima

- Pilih dua bilangan prima besar, p dan q .
- Bilangan ini harus cukup besar untuk menjamin keamanan, biasanya minimal 1024 bit.

Perhitungan Modulus dan Totien

- Hitung $n = p \times q$, yang digunakan sebagai modulus untuk kunci publik dan privat.
- Hitung totien Euler: $\phi(n) = (p - 1) \times (q - 1)$

Penentuan Kunci Publik (e)

- Pilih bilangan bulat e sedemikian sehingga $1 < e < \phi(n)$ dan $\gcd(e, \phi(n)) = 1$.
 - Nilai e menjadi eksponen kunci publik.
- Penentuan Kunci Privat (d)
- Hitung d sebagai invers modulo dari e terhadap $\phi(n)$, sehingga: $d \times e \equiv 1 \pmod{\phi(n)}$
 - Nilai d menjadi eksponen kunci privat.
- Enkripsi dan Dekripsi
- Untuk mengirim pesan M , enkripsi menggunakan kunci publik: $C \equiv M^e \pmod{n}$
 - Penerima mendekripsi menggunakan kunci privat: $M \equiv C^d \pmod{n}$
- Digital Signature
- Untuk menandatangani pesan M , pengirim menghitung tanda tangan: $S \equiv M^d \pmod{n}$
 - Penerima memverifikasi dengan kunci publik: $M \equiv S^e \pmod{n}$
 - Jika hasil verifikasi cocok dengan pesan asli, konten dianggap autentik.

2.4 Tahapan Penelitian

Tahapan penelitian dilakukan secara sistematis agar model yang dikembangkan dapat diuji secara terukur. Tahapan penelitian meliputi studi literatur, identifikasi kebutuhan model, pengumpulan file multimedia, perancangan model digital signature RSA, implementasi proses hashing, signing, dan verification, pengujian file asli dan file manipulasi, analisis hasil pengujian, serta penyusunan laporan dan luaran penelitian. Adapun secara jelas dapat dilihat pada gambar berikut:



Gambar 1. Tahapan Penelitian

Pada gambar 1 diatas dapat dilihat terhadap tahapan yang dilalui pada penelitian. Penjelasan secara ringkas dapat dilihat berikut:

- Studi literatur dan gap penelitian**
Peneliti mengkaji teori multimedia, kriptografi, digital signature, algoritma RSA, fungsi hash, dan penelitian terdahulu. Tahap ini bertujuan menemukan gap penelitian dan memperkuat dasar ilmiah penelitian.
- Identifikasi kebutuhan model**
Peneliti menentukan kebutuhan model yang akan dikembangkan, seperti jenis file multimedia, format file, ukuran file, fungsi hash, proses signing, proses verification, dan parameter pengujian.
- Pengumpulan file multimedia**
Peneliti menyiapkan file multimedia sebagai objek uji. File yang digunakan meliputi gambar, audio, dan video dengan format JPEG, PNG, MP3, WAV, MP4, dan AVI.
- Perancangan model RSA digital signature**
Peneliti merancang alur kerja model digital signature berbasis RSA. Model ini mencakup proses pembentukan hash, penandatanganan menggunakan kunci privat, dan verifikasi menggunakan kunci publik.
- Implementasi hashing, signing, verification**
Peneliti menerapkan proses teknis pada model yang telah dirancang. File multimedia diproses untuk menghasilkan hash, kemudian ditandatangani dan diverifikasi menggunakan algoritma RSA.
- Pengujian file asli dan manipulasi**
Peneliti menguji file asli dan file yang telah dimanipulasi. Pengujian ini bertujuan mengetahui kemampuan model dalam membedakan file yang masih asli dan file yang telah berubah.
- Analisis hasil pengujian**
Peneliti menganalisis hasil verifikasi, nilai hash, waktu signing, waktu verification, dan status validitas file. Tahap ini digunakan untuk menilai efektivitas model dalam menjamin keaslian dan integritas konten multimedia.

h. Penyusunan laporan dan luaran

Peneliti menyusun laporan akhir penelitian berdasarkan hasil pengujian dan analisis. Luaran yang ditargetkan meliputi model digital signature RSA, laporan penelitian, dan artikel ilmiah.

2.5 Parameter Pengukuran dan Pengamatan

Parameter pengukuran dan pengamatan digunakan untuk menilai kemampuan model dalam menjamin keaslian dan integritas file multimedia. Parameter yang diamati meliputi jenis file, format file, ukuran file, nilai hash, waktu signing, waktu verifikasi, status verifikasi, dan kemampuan deteksi manipulasi ataupun dapat dilihat pada tabel 1 berikut:

Tabel 1. Parameter Pengukuran

No	Parameter	Indikator Pengukuran	Satuan/Keluaran
1	Jenis file multimedia	Format file yang diuji	JPEG, PNG, MP3, WAV, MP4, AVI
2	Ukuran file	Besaran file multimedia	KB atau MB
3	Nilai hash	Perubahan nilai hash sebelum dan sesudah manipulasi	Sama atau berbeda
4	Status digital signature	Hasil proses verifikasi	Valid atau tidak valid
5	Waktu signing	Lama proses pembentukan tanda tangan digital	Detik atau milidetik
6	Waktu verifikasi	Lama proses validasi tanda tangan digital	Detik atau milidetik
7	Deteksi manipulasi	Kemampuan model mendeteksi perubahan file	Terdeteksi atau tidak terdeteksi
8	Tingkat keberhasilan verifikasi	Jumlah file yang berhasil diverifikasi dengan benar	Persentase

Tingkat keberhasilan verifikasi dapat dihitung dengan rumus berikut:

$$\text{Tingkat Keberhasilan Verifikasi} = \frac{\text{Jumlah File yang Terverifikasi dengan Benar}}{\text{Jumlah Seluruh File Uji}} * 100\% \quad (1)$$

Waktu rata-rata signing dapat dihitung dengan rumus berikut:

$$\text{Rata – Rata Waktu Signing} = \frac{\text{Total Waktu Signing}}{\text{Jumlah File Uji}} \quad (2)$$

Waktu rata-rata verifikasi dapat dihitung dengan rumus berikut:

$$\text{Rata – Rata Waktu Verifikasi} = \frac{\text{Total Waktu Verifikasi}}{\text{Jumlah File Uji}} \quad (3)$$

3. HASIL DAN PEMBAHASAN

3.1 Analisis Masalah

Perkembangan teknologi multimedia memungkinkan konten digital berupa citra, audio, dan video dibuat, disimpan, serta didistribusikan dengan mudah. Namun, kemudahan tersebut juga menimbulkan permasalahan terkait keaslian dan integritas konten digital. Berkas multimedia dapat disalin, diubah, dikompresi, atau dimanipulasi tanpa sepengetahuan pemilik aslinya. Perubahan tersebut tidak selalu mudah dikenali melalui pemeriksaan visual atau pendengaran, terutama apabila perubahan dilakukan pada bagian tertentu dari berkas.

Permasalahan utama dalam penelitian ini adalah bagaimana memastikan bahwa berkas multimedia yang diterima masih sesuai dengan berkas yang telah ditandatangani sebelumnya. Pemeriksaan secara manual memiliki keterbatasan karena tidak memberikan bukti kriptografis yang memadai mengenai integritas berkas. Oleh karena itu, diperlukan mekanisme yang mampu mendeteksi perubahan data dan memverifikasi tanda tangan digital secara sistematis.

Penelitian ini menggunakan algoritma RSA (Rivest–Shamir–Adleman) dalam mekanisme digital signature. Proses dimulai dengan menghitung nilai hash berkas multimedia menggunakan SHA-256. Nilai hash tersebut kemudian ditandatangani menggunakan kunci privat RSA. Pada tahap verifikasi, sistem menggunakan kunci publik untuk memeriksa tanda tangan digital dan memastikan kesesuaian berkas dengan data yang ditandatangani. Apabila isi berkas berubah setelah penandatanganan, verifikasi diharapkan menghasilkan status tidak valid. Pengujian dirancang menggunakan enam format multimedia, yaitu JPEG dan PNG untuk citra, MP3 dan WAV untuk audio, serta MP4 dan AVI untuk video. Parameter yang diamati meliputi jenis file, ukuran file, nilai hash, status digital signature, waktu signing, waktu verifikasi, deteksi manipulasi, dan tingkat keberhasilan verifikasi.

3.2 Implementasi Digital Signature Berbasis RSA

Implementasi digital signature dirancang melalui tiga tahapan utama, yaitu pembentukan tanda tangan digital, penyimpanan tanda tangan, dan verifikasi keaslian berkas. Pada tahap penandatanganan, sistem membaca berkas multimedia dan menghitung nilai hash menggunakan SHA-256. Nilai hash kemudian ditandatangani menggunakan kunci privat RSA sehingga menghasilkan tanda tangan digital yang berkaitan dengan isi berkas tersebut.

Pada tahap verifikasi, sistem membaca kembali berkas multimedia dan memeriksa tanda tangan menggunakan kunci publik RSA sesuai skema tanda tangan yang digunakan. Verifikasi juga memastikan bahwa isi berkas yang diperiksa sesuai dengan isi berkas yang ditandatangani. Jika verifikasi berhasil, berkas dinyatakan valid. Sebaliknya, jika berkas mengalami perubahan atau tanda tangan tidak sesuai, sistem memberikan status tidak valid.

Pengujian dirancang mencakup enam format berkas multimedia. Untuk memberikan gambaran mengenai penyajian hasil, Tabel 2 menampilkan ukuran berkas dan waktu pemrosesan.

Tabel 2. Waktu Penandatanganan dan Verifikasi

No	Format	Ukuran File (MB)	Waktu Signing (Detik)	Waktu Verifikasi (Detik)
1	JPEG	2,50	0,012	0,004
2	PNG	4,20	0,015	0,005
3	MP3	5,80	0,016	0,005
4	WAV	18,60	0,021	0,006
5	MP4	45,30	0,029	0,008
6	AVI	82,70	0,038	0,010
Total	-	159,10	0,131	0,038
Rata – Rata	-	26,52	0,0218	0,0063

Berdasarkan tabel 2, waktu signing berada pada rentang 0,012–0,038 detik, sedangkan waktu verifikasi berada pada rentang 0,004–0,010 detik. Berkas JPEG memiliki waktu pemrosesan terendah, sedangkan AVI memiliki waktu pemrosesan tertinggi. Pola tersebut memberikan hasil bahwa berkas berukuran lebih besar berpotensi membutuhkan waktu pemrosesan lebih lama. Namun, hubungan ini belum dapat dinyatakan sebagai temuan penelitian sebelum dilakukan pengujian aktual. Waktu pemrosesan juga dipengaruhi oleh proses hashing, implementasi algoritma, ukuran kunci RSA, perangkat keras, dan pustaka kriptografi yang digunakan.

3.3 Pengujian Keaslian dan Integritas Berkas Multimedia

Pengujian integritas dilakukan dengan membandingkan hasil verifikasi berkas asli dan berkas yang telah dimodifikasi. Berkas asli ditandatangani terlebih dahulu, kemudian diverifikasi menggunakan tanda tangan digital yang dihasilkan. Selanjutnya, isi berkas diubah dan proses verifikasi diulang menggunakan tanda tangan yang sama.

Tabel 3. Hasil Verifikasi Keaslian Berkas

No	Format	Kondisi Berkas	Status Verifikasi	Hasil Deteksi
1	JPEG	Asli	Valid	Sesuai
2	JPEG	Termodifikasi	Tidak Valid	Terdeteksi
3	PNG	Asli	Valid	Sesuai
4	PNG	Termodifikasi	Tidak Valid	Terdeteksi
5	MP3	Asli	Valid	Sesuai
6	MP3	Termodifikasi	Tidak Valid	Terdeteksi
7	WAV	Asli	Valid	Sesuai
8	WAV	Termodifikasi	Tidak Valid	Terdeteksi
9	MP4	Asli	Valid	Sesuai
10	MP4	Termodifikasi	Tidak Valid	Terdeteksi
11	AVI	Asli	Valid	Sesuai
12	AVI	Termodifikasi	Tidak Valid	Terdeteksi

Pada skenario tabel 3, enam berkas asli dinyatakan valid dan enam berkas termodifikasi dinyatakan tidak valid. Jika hasil yang sama diperoleh melalui pengujian aktual, hal ini menunjukkan bahwa sistem mampu membedakan berkas yang masih sesuai dengan data yang ditandatangani dari berkas yang telah mengalami perubahan. Secara konseptual, perubahan isi berkas menyebabkan nilai hash hasil perhitungan ulang berbeda dari nilai hash yang ditandatangani sebelumnya. Ketidaksesuaian tersebut menyebabkan proses verifikasi gagal. Mekanisme ini mendukung pemeriksaan integritas karena perubahan data dapat dideteksi tanpa harus membandingkan berkas secara manual.

Nilai hash dapat digunakan untuk mengamati perubahan isi berkas. Tabel 4 memperlihatkan bentuk pencatatan nilai hash sebelum dan sesudah manipulasi. Nilai berikut format penyajian dan bukan hash yang dihitung dari berkas nyata.

Tabel 4. Perubahan Nilai Hash Berkas Multimedia

No.	Format	Hash sebelum manipulasi	Hash setelah manipulasi	Perbandingan
1	JPEG	a1b2c3...	d4e5f6...	Berbeda
2	PNG	b2c3d4...	e5f6a7...	Berbeda
3	MP3	c3d4e5...	f6a7b8...	Berbeda
4	WAV	d4e5f6...	a7b8c9...	Berbeda
5	MP4	e5f6a7...	b8c9d0...	Berbeda
6	AVI	f6a7b8...	c9d0e1...	Berbeda

Tabel 4 tersebut menunjukkan bentuk perbedaan yang perlu dicatat pada pengujian. Untuk pelaporan ilmiah, nilai hash harus diambil langsung dari keluaran program dan ditampilkan secara lengkap atau dengan pemotongan yang dijelaskan secara konsisten. Apabila hash berubah setelah manipulasi, hal tersebut mendukung indikasi bahwa isi berkas berbeda. Keputusan valid atau tidak valid tetap ditentukan melalui verifikasi tanda tangan digital, bukan hanya berdasarkan tampilan nilai hash.

3.4 Analisis Waktu Penandatanganan dan Verifikasi

Waktu signing dan verifikasi digunakan untuk mengevaluasi efisiensi penerapan digital signature RSA pada berkas multimedia. Signing melibatkan perhitungan hash dan pembentukan tanda tangan menggunakan kunci privat. Verifikasi melibatkan pemeriksaan tanda tangan menggunakan kunci publik serta penghitungan hash berkas yang diperiksa. Berdasarkan angka pada Tabel 2, jumlah waktu signing keenam berkas adalah 0,131 detik. Dengan jumlah enam berkas. Sementara itu, jumlah waktu verifikasi keenam berkas adalah 0,038 detik.

Tabel 5. Ringkasan Waktu Pemrosesan

Parameter	Total Waktu (Detik)	Jumlah Berkas	Rata-Rata (Detik)
Signing	0,131	6	0,0218
Verifikasi	0,038	6	0,0063

Berdasarkan perhitungan rata-rata waktu signing sebesar 0,0218 detik dan rata-rata waktu verifikasi sebesar 0,0063 detik. Verifikasi memerlukan waktu lebih singkat dibandingkan signing. Akan tetapi, perbedaan tersebut belum dapat digeneralisasi sebagai karakteristik pasti sistem yang diteliti karena belum diukur melalui program aktual. Pengukuran aktual sebaiknya dilakukan berulang pada perangkat dan konfigurasi yang sama. Setiap pengujian perlu mencatat ukuran kunci RSA, algoritma hash, pustaka kriptografi, spesifikasi perangkat keras, serta jumlah pengulangan. Pengulangan sebanyak 30 kali per skenario dapat digunakan untuk menghitung rata-rata dan simpangan baku agar variasi waktu pemrosesan dapat dianalisis.

Ukuran berkas juga perlu diperhatikan karena proses hashing terhadap berkas yang lebih besar umumnya memerlukan pemrosesan data lebih banyak. Namun, untuk mengisolasi pengaruh ukuran berkas, diperlukan pengujian dengan ukuran yang bervariasi dan faktor lainnya dikendalikan. Dengan demikian, kesimpulan mengenai hubungan ukuran berkas dan waktu pemrosesan dapat didasarkan pada hasil pengukuran

3.5 Analisis Kemampuan Deteksi Manipulasi

Kemampuan mendeteksi manipulasi merupakan aspek penting dalam evaluasi digital signature. Tanda tangan digital digunakan untuk memeriksa apakah berkas yang diterima masih sesuai dengan isi berkas yang ditandatangani. Ketika isi berkas berubah, proses verifikasi seharusnya gagal karena data yang diperiksa tidak lagi sesuai dengan tanda tangan yang dibuat sebelumnya. efinsi keberhasilan pada rumus tersebut mencakup dua kondisi: berkas asli dinyatakan valid dan berkas termodifikasi dinyatakan tidak valid. Dengan demikian, keberhasilan tidak hanya dinilai dari diterimanya berkas asli, tetapi juga dari ditolakanya berkas yang telah dimanipulasi. Berdasarkan Tabel 3, dalam skenario terdapat 12 hasil pengujian yang sesuai dengan kondisi yang diharapkan dari total 12 pengujian.

3.6 Implikasi Hasil Penelitian

Penerapan digital signature berbasis RSA berpotensi menjadi mekanisme verifikasi integritas bagi berbagai jenis konten multimedia, termasuk citra, audio, dan video. Penggunaan mekanisme yang sama pada berbagai format dapat membantu menyederhanakan proses verifikasi karena sistem berfokus pada isi berkas dan tanda tangan digital, bukan pada pemeriksaan manual terhadap konten. Dalam konteks distribusi konten digital, mekanisme ini dapat dimanfaatkan untuk membantu memeriksa apakah berkas yang diterima masih sesuai dengan berkas yang ditandatangani oleh pembuatnya. Penerapan tersebut relevan untuk arsip digital, dokumen multimedia, materi pembelajaran, dan pertukaran konten digital. Meskipun demikian, digital signature tidak mencegah seseorang

mengubah atau menyalin berkas. Mekanisme ini membantu mendeteksi ketidaksesuaian antara berkas yang diperiksa dan data yang ditandatangani. Untuk memastikan identitas penanda tangan, kunci publik harus dapat dikaitkan dengan identitas pemilik yang tepercaya, misalnya melalui sertifikat digital atau mekanisme pengelolaan kunci yang sesuai.

Implementasi RSA juga perlu menggunakan skema tanda tangan digital yang aman melalui pustaka kriptografi teruji. Penggunaan SHA-256 dan skema tanda tangan seperti RSA-PSS dapat dipertimbangkan. Verifikasi harus dilakukan terhadap tanda tangan digital yang valid, bukan hanya dengan mengasumsikan bahwa hasil operasi RSA langsung menghasilkan nilai hash yang sama. Selain aspek keamanan, pengukuran waktu pemrosesan diperlukan untuk mengetahui karakteristik kinerja sistem. Pengujian pada citra, audio, dan video dengan ukuran beragam dapat memberikan gambaran tentang efisiensi proses signing dan verifikasi. Namun, implikasi empiris mengenai keandalan dan efisiensi sistem baru dapat ditetapkan setelah pengujian aktual dilakukan.

3.7 Pembahasan

Hasil penelitian ini menunjukkan bahwa penerapan digital signature berbasis algoritma Rivest–Shamir–Adleman (RSA) yang dikombinasikan dengan fungsi hash SHA-256 dapat digunakan sebagai pendekatan untuk memverifikasi integritas dan keaslian berkas multimedia. Model yang dirancang menerapkan proses pembentukan nilai hash dari berkas, penandatanganan menggunakan kunci privat RSA, serta verifikasi menggunakan kunci publik. Mekanisme tersebut memungkinkan sistem memeriksa apakah berkas yang diterima masih sesuai dengan berkas yang telah ditandatangani sebelumnya. Apabila isi berkas mengalami perubahan, nilai hash yang dihitung kembali akan berbeda sehingga tanda tangan digital tidak lagi sesuai dengan konten yang diverifikasi.

Pengujian dalam penelitian ini dirancang terhadap enam format multimedia, yaitu JPEG dan PNG untuk citra, MP3 dan WAV untuk audio, serta MP4 dan AVI untuk video. Pemilihan format tersebut dimaksudkan untuk menggambarkan penerapan mekanisme verifikasi pada berkas dengan karakteristik dan ukuran yang berbeda. Berdasarkan data skenario pada Tabel 2, ukuran berkas berada pada rentang 2,50–82,70 MB, dengan waktu signing antara 0,012–0,038 detik dan waktu verifikasi antara 0,004–0,010 detik. Waktu rata-rata signing tercatat sebesar 0,0218 detik, sedangkan waktu rata-rata verifikasi sebesar 0,0063 detik. Secara deskriptif, angka tersebut menunjukkan bahwa proses verifikasi memiliki waktu pemrosesan lebih rendah dibandingkan proses penandatanganan pada skenario yang disajikan. Meskipun demikian, angka tersebut belum dapat digunakan untuk menyimpulkan kinerja empiris sistem karena masih memerlukan pengukuran langsung melalui implementasi program dan pengujian berulang pada lingkungan perangkat keras serta konfigurasi kriptografi yang terkontrol.

Dari aspek integritas berkas, Tabel 3 memperlihatkan skenario pengujian terhadap 12 kondisi, yang terdiri atas enam berkas asli dan enam berkas termodifikasi. Dalam skenario tersebut, seluruh berkas asli dinyatakan valid, sedangkan seluruh berkas termodifikasi dinyatakan tidak valid. Dengan demikian, tingkat keberhasilan verifikasi yang diperoleh berdasarkan skenario adalah 100%. Hasil ini menggambarkan kondisi yang diharapkan dari penerapan digital signature, yaitu berkas yang tidak berubah setelah ditandatangani dapat diverifikasi, sedangkan berkas yang mengalami perubahan ditolak oleh sistem. Namun, angka 100% tersebut tidak dapat diinterpretasikan sebagai tingkat keberhasilan eksperimen aktual karena hasil pengujian yang disajikan masih bersifat skenario. Validasi empiris perlu dilakukan dengan menjalankan proses signing dan verifikasi terhadap berkas nyata, kemudian mencatat keluaran program untuk setiap kondisi pengujian.

Perubahan nilai hash sebagaimana ditunjukkan pada Tabel 4 juga menjelaskan hubungan antara fungsi hash SHA-256 dan mekanisme deteksi manipulasi. Fungsi hash menghasilkan nilai ringkasan berdasarkan isi berkas yang diproses. Ketika isi berkas berubah, hasil perhitungan hash diharapkan berbeda dari nilai hash sebelumnya. Ketidaksesuaian tersebut menjadi dasar untuk mendeteksi bahwa berkas yang diperiksa tidak lagi identik dengan berkas yang ditandatangani. Meskipun demikian, nilai hash yang dicantumkan dalam tabel masih berupa ilustrasi dan bukan keluaran perhitungan dari berkas multimedia aktual. Oleh sebab itu, penelitian lanjutan perlu mencatat nilai hash SHA-256 secara lengkap dari setiap berkas sebelum dan sesudah manipulasi serta menyimpan hasil verifikasi tanda tangan digital sebagai bukti pengujian yang dapat direproduksi.

Jika dibandingkan dengan penelitian Hutagalung, Ramadhan, dan Sihombing [2] mengenai keamanan data menggunakan SHA-256 dan RSA pada digital signature, penelitian ini memiliki kesamaan dalam penggunaan fungsi hash dan kriptografi kunci publik untuk mendukung integritas serta autentikasi data. Kesamaan tersebut terletak pada prinsip bahwa data diringkas menggunakan fungsi hash, kemudian tanda tangan digital diverifikasi menggunakan mekanisme kriptografi yang sesuai. Perbedaannya, penelitian ini menempatkan berkas multimedia sebagai objek kajian dengan mencakup enam format citra, audio, dan video. Dengan demikian, fokus penelitian tidak hanya pada mekanisme keamanan data secara umum, tetapi juga pada rancangan pengujian yang mempertimbangkan variasi format dan ukuran berkas multimedia. Meskipun demikian, perbedaan tersebut menunjukkan ruang lingkup kajian yang berbeda dan belum dapat dijadikan bukti bahwa model yang dikembangkan memiliki kinerja lebih baik daripada penelitian terdahulu.

Penelitian Nuraeni, Kurniadi, dan Rahayu [3] membahas implementasi RSA dan AES-128 dalam skema digital signature berbasis QR Code untuk legalisasi dokumen. Penelitian tersebut relevan sebagai pembanding karena sama-sama mengkaji penerapan kriptografi untuk mendukung autentikasi dan perlindungan keaslian dokumen digital. Perbedaan utamanya terletak pada orientasi penerapan. Penelitian Nuraeni dan rekan-rekan berfokus pada skema legalisasi dokumen berbasis QR Code dengan kombinasi RSA dan AES-128, sedangkan penelitian ini merancang mekanisme verifikasi integritas berkas multimedia menggunakan RSA dan SHA-256. Objek pengujian penelitian ini mencakup citra, audio, dan video, sehingga model yang diusulkan diarahkan pada pemeriksaan perubahan isi berkas tanpa bergantung pada satu jenis dokumen saja. Perbedaan tersebut memperlihatkan variasi pendekatan dalam penerapan kriptografi, bukan keunggulan komparatif yang telah dibuktikan melalui pengujian langsung.

Selain kedua penelitian tersebut, Al Fatah, Akbi, dan Muthohirin [1] membahas peningkatan kinerja steganografi LSB melalui penggunaan RSA dan Huffman. Penelitian tersebut memiliki keterkaitan dalam penggunaan algoritma RSA untuk mendukung keamanan konten digital. Akan tetapi, tujuan penerapannya berbeda. Penelitian tersebut berorientasi pada peningkatan kinerja steganografi, sedangkan penelitian ini berfokus pada verifikasi integritas dan deteksi perubahan berkas melalui digital signature. Dengan demikian, kontribusi yang ditawarkan penelitian ini terletak pada penggunaan tanda tangan digital sebagai mekanisme pemeriksaan keaslian dan integritas konten multimedia, bukan pada penyembunyian pesan atau peningkatan kapasitas steganografi.

Berdasarkan perbandingan tersebut, kontribusi utama penelitian ini adalah perancangan model digital signature berbasis RSA dan SHA-256 yang diarahkan untuk memverifikasi enam format multimedia dalam satu kerangka pengujian. Model tersebut menghubungkan tahapan pembentukan hash, penandatanganan, verifikasi, dan pengamatan waktu pemrosesan serta deteksi manipulasi. Pendekatan ini dapat menjadi dasar bagi pengembangan aplikasi verifikasi berkas multimedia pada lingkungan pendidikan, pengarsipan digital, dan distribusi konten. Namun, klaim mengenai efisiensi, tingkat keberhasilan, dan keandalan model harus didasarkan pada pengujian aktual, bukan semata-mata pada nilai yang disajikan dalam skenario.

Secara keseluruhan, pembahasan menunjukkan bahwa kombinasi RSA dan SHA-256 secara konseptual sesuai untuk mendukung pemeriksaan integritas konten multimedia. Agar hasil penelitian memiliki kekuatan empiris yang memadai, implementasi berikutnya perlu menggunakan pustaka kriptografi yang teruji dan skema tanda tangan digital yang aman, seperti RSA-PSS. Pengujian juga perlu dilakukan berulang pada setiap format dengan mencatat ukuran kunci, spesifikasi perangkat keras, konfigurasi perangkat lunak, waktu pemrosesan, serta hasil verifikasi. Selain itu, identitas penanda tangan perlu dikaitkan dengan kunci publik tepercaya agar autentikasi tidak hanya bergantung pada keberhasilan matematis proses verifikasi. Dengan langkah tersebut, efektivitas model dalam mendeteksi manipulasi dan karakteristik kinerjanya dapat dinilai secara objektif serta dibandingkan secara lebih adil dengan penelitian terdahulu.

4. KESIMPULAN

Penelitian ini membahas penerapan digital signature berbasis algoritma RSA untuk menjamin keaslian dan integritas konten multimedia. Model yang dirancang mengintegrasikan proses hashing menggunakan SHA-256, penandatanganan dengan kunci privat RSA, dan verifikasi menggunakan kunci publik. Pengujian direncanakan pada 6 format multimedia, yaitu JPEG, PNG, MP3, WAV, MP4, dan AVI, dengan parameter berupa ukuran file, nilai hash, status verifikasi, waktu signing, waktu verifikasi, serta kemampuan mendeteksi manipulasi. Berdasarkan skenario perhitungan, ukuran file yang digunakan berada pada rentang 2,50–82,70 MB. Waktu signing berkisar antara 0,012–0,038 detik, dengan rata-rata 0,0218 detik, sedangkan waktu verifikasi berkisar antara 0,004–0,010 detik, dengan rata-rata 0,0063 detik. Pada pengujian integritas terhadap 12 kondisi, yang terdiri atas 6 file asli dan 6 file termodifikasi, seluruh hasil diasumsikan sesuai dengan kondisi yang diharapkan sehingga menghasilkan tingkat keberhasilan verifikasi sebesar 100%. Perubahan nilai hash juga digunakan sebagai indikator awal untuk mengidentifikasi perubahan isi file setelah manipulasi. Secara konseptual, hasil tersebut menggambarkan potensi digital signature RSA dalam mendukung pemeriksaan integritas konten multimedia melalui mekanisme verifikasi kriptografis. Penelitian selanjutnya perlu menguji berbagai ukuran file secara berulang, mencatat spesifikasi perangkat dan konfigurasi kunci RSA, serta menerapkan skema tanda tangan digital yang aman. Dengan demikian, efektivitas dan efisiensi model dalam mendeteksi manipulasi pada berbagai format multimedia dapat dievaluasi secara objektif.

REFERENCES

- [1] M. R. A. G. Al Fatah, D. R. Akbi, and B. F. Muthohirin, "Enhancing The Performance of LSB Steganography with RSA and Huffman," *J. ELTIKOM*, vol. 10, no. 1, pp. 47–62, 2026, doi: 10.31961/eltikom.v10i1.2022.
- [2] J. Hutagalung, P. S. Ramadhan, and S. J. Sihombing, "Keamanan Data Menggunakan Secure Hashing Algorithm (SHA-256) dan Rivest Shamir Adleman (RSA) pada Digital Signature," *J. Teknol. Inf. dan Ilmu Komput.*, vol. 10, no. 6, pp. 1213–1222, 2023, doi: 10.25126/jtiik.2023107319.



- [3] F. Nuraeni, D. Kurniadi, and D. N. Rahayu, "Implementation of RSA and AES-128 Super Encryption on QR-Code Based Digital Signature Schemes for Document Legalization," *J. Tek. Inform.*, vol. 5, no. 3, pp. 675–684, 2024, doi: 10.52436/1.jutif.2024.5.3.1426.
- [4] A. R. Nurjaman, "A digital document tracker on a file storage system uses a combination of the SHA3-512 and RSA algorithms to safeguard the authenticity of document data," *J. Ilm. Teknol. Inf. Terap.*, vol. 10, no. 3, 2024, doi: 10.33197/jitter.vol10.iss3.2024.2200.
- [5] E. N. Nur'allifa, R. R. J. Putra, and M. Nursalman, "RSA Blind Signature sebagai dasar pengamanan pada sistem e-voting dengan Prinsip Frictionless User," *J. Komput. Teknol. Inf. Sist. Komput.*, vol. 4, no. 2, 2025, doi: 10.62712/juktisi.v4i2.527.
- [6] Y. Lubis, I. Rusydi, and A. H. Elyas, "Implementasi Algoritma Kriptografi Tanda Tangan Digital QR-Code Pada Dokumen dengan Metode RSA," *War. Dharmawangsa*, vol. 18, no. 4, pp. 1429–1439, 2024, doi: 10.46576/wdw.v18i4.5247.
- [7] G. K. S. Artajaya and A. Muliantara, "Impelementasi Kriptografi RSA dan XOR Cipher untuk Enkripsi Citra Digital KTP," *J. Nas. Teknol. Inf. dan Apl.*, vol. 2, no. 4, pp. 665–672, 2024, doi: 10.24843/JNATIA.2024.v02.i04.p01.
- [8] N. P. Utomo and T. Haryanti, "equirement Engineering Sistem Kriptografi RSA pada Gmail," *Comput. Insight J. Comput. Sci.*, vol. 4, no. 2, pp. 40–46, 2024, doi: 10.30651/comp_insight.v4i2.21735.
- [9] M. Hadi, H. Mulyo, and T. Tamrin, "Performance Analysis of RSA and AES Algorithms in Digital Image Encryption," *JTINFO J. Tek. Inform.*, vol. 4, no. 1, pp. 197–207, 2025, doi: <https://doi.org/10.25126/jtiik.2023107319>.
- [10] N. H. Sari, "Penerapan Teknik Digital Signature Dalam Pengamanan Piagam Penghargaan Menggunakan Algoritma SHA-1 dan RSA," *Manag. Inf. Syst. J.*, vol. 2, no. 3, pp. 55–67, 2024, doi: <https://doi.org/10.47065/mis.v2i3.1465>.
- [11] F. Az-Zahra, R. Marwati, and R. Sispiyati, "Implementasi QR Code dengan Algoritma Secure Hash Algorithm (SHA)-256 dan Rivest Shamir Adleman (RSA) yang Ditingkatkan untuk Autentikasi Dokumen Digital," *J. EurekaMatika*, vol. 12, no. 1, pp. 11–22, 2024, doi: <https://doi.org/10.17509/jem.v12i1.67161>.
- [12] E. P. Nugroho, I. Afrianto, and R. N. Sukmana, "Pengukuran Kelayakan Simulator Forensik Digital Menggunakan Metode Multimedia Mania," *MATRIK J. Manajemen, Tek. Inform. dan Rekayasa Komput.*, vol. 21, no. 2, pp. 351–366, 2022, doi: <https://doi.org/10.30812/matrik.v21i2.1556>.
- [13] H. Putri, L. Virna, T. Febrianti, and T. Sutabri, "Pengamanan Data Transmisi Aplikasi Web Menggunakan Algoritma Kriptografi RSA: Studi Kasus dan Analisis," *MIFORTECH J. Manaj. Inform. dan Teknol.*, vol. 5, no. 1, pp. 153–170, 2025, doi: <https://doi.org/10.51903/rdsne23>.
- [14] Sugiyatno and H. M. Rahman, "Analisis Kinerja AES dan RC6 pada File Multimedia," *J. Sains Teknol. dan Sist. Inf.*, vol. 6, no. 1, pp. 46–51, 2026, doi: <https://doi.org/10.54259/satesi.v6i1.7523>.
- [15] R. A. Iswandi, D. Sarumaha, and S. Amir, "Analisis Performa Kecepatan Algoritma Dual Modulus RSA dalam Pengamanan Data Teks dengan Python," *J. Inform. dan Sains Teknol.*, vol. 4, no. 2, pp. 1–10, 2026, doi: <https://doi.org/10.62951/modem.v4i2.842>.
- [16] T. M. Aziz and S. Dwiasnati, "Letter Numbering and Storage Application with WEB-based AES and RSA methods," *J. Tata Kelola dan Kerangka Kerja Teknol. Inf.*, vol. 9, no. 1, pp. 1–8, 2023, doi: <https://doi.org/10.34010/jtk3ti.v9i1.8025>.
- [17] M. R. Syifauddin, R. H. Kusumodestoni, and Sarwido, "Penerapan Algoritma Rivest Shamir Aldeman (RSA) untuk Pengamanan Data Gambar Nasabah BMT Al-Hikmah Permata," *J. dan Penelit. Manaj. Inform.*, vol. 3, no. 1, pp. 726–741, 2024, doi: DOI: 10.33395/jmp.v13i1.13805.
- [18] C. Repi, J. Titaley, and E. Ketaren, "Implementasi Kriptografi Dalam Pengamanan Data Gambar Menggunakan Algoritma RSA," *J. TIMES*, vol. 13, no. 1, pp. 93–99, 2024, doi: <https://doi.org/10.51351/jtm.13.1.2024750>.
- [19] P. Apriani, A. H. Hasugian, and I. Rusydi, "Teknik Steganografi Discrete Cosine Transform Dan Algoritma Rsa Untuk Menyisipkan Pesan Pada Audio," *Jar. Sist. Inf. Robot.*, vol. 8, no. 1, pp. 1–9, 2024, doi: <https://doi.org/10.58486/jsr.v8i1.319>.
- [20] A. Rahayu, A. P. Ardana, C. Pramudhita, D. Syafitri, and R. Z. Siregar, "Comparison of algorithm RSA with algorithm Blowfish in Data Security Application Design," *J. Math. Technol.*, vol. 3, no. 2, pp. 213–219, 2024, doi: <https://doi.org/10.63893/matech.v3i2.224>.